Alma Mater Studiorum · Università di Bologna

FACOLTÀ DI SCIENZE MATEMATICHE, FISICHE E NATURALI
Corso di Laurea in Scienze di Internet

I PROFILI GIURIDICI DELL'ATTIVITA' DI CONTROLLO CON MEZZI INFORMATICI SUI LAVORATORI

Tesi di Laurea in Diritto di Internet

Relatore:
Chiar.ma Prof.ssa
Giusella Finocchiaro

Correlatore:
Chiar.mo Prof.
Edoardo Mollona

Presentata da:
Luca Peloncini

Sessione I
Anno Accademico 2009-2010

Ai miei genitori...

Introduzione

Agli inizi del Novecento, il controllo gerarchico dei dipendenti era la caratteristica principale dell'impresa e creava una totale mancanza di attenzione verso gli aspetti psicologici del lavoro. Successivamente, con il progresso tecnologico, la prestazione lavorativa ha subito un forte cambiamento creandosi nuovi modelli economici come la knowledge economy: l'informazione, la conoscenza, le relazioni e i mezzi di comunicazione ne sono divenute il fondamento. Al giorno d'oggi, infatti, la velocità di innovazione impone l'aggiornamento costante della competenza professionale dei lavoratori. La knowledge economy mette in discussione le grandi concentrazioni di potere e il lavoratore non viene più visto come un ingranaggio del sistema di produzione; al lavoratore viene concessa più autonomia, creatività e libertà relazionale che porta benefici all'impresa, ma è anche argomento di discussione il potere di controllo messo in atto dal datore di lavoro per garantire la corretta esecuzione della prestazione lavorativa dei propri dipendenti.
In particolare, si esamineranno le normative che regolano l'utilizzo della nuova tecnologia fondamentale delle aziende: Internet, che è una concreta risorsa per un notevole incremento di efficienza e velocità nell'attuazione delle funzioni lavorative. La gestione della connessione ad Internet all'interno di una prestazione lavorativa, come l'utilizzo della posta elettronica e la navigazione in rete, sono divenute materia di confronto, in quanto vi è da una parte il legittimo potere di controllo del datore di lavoro e dall'altra i diritti del lavoratore. Per questo motivo verrà analizzata, la legittimità dell'uso di sistemi elettronici che permettano di effettuare controlli specifici sul comportamento

del lavoratore; in altre parole, l'implicazione del lavoratore nello svolgimento della prestazione determina il rischio che il controllo preso in esame sia esercitato in modo lesivo di beni fondamentali quali, in primis, la dignità e la riservatezza del lavoratore medesimo.

A fronte della mancanza di una normativa specifica di riferimento, il problema rimane apertissimo come dimostrano i contrasti esistenti tra la dottrina nettamente orientata verso le esigenze garantiste di tutela del lavoratore contro l'invasività dei controlli tecnologici datoriali e la giurisprudenza viceversa maggiormente incline a legittimare i controlli delle aziende.

In particolare, un problema oggetto di acceso dibattito in Italia e in Europa è stato quello del controllo a distanza dei lavoratori, che si realizza monitorando le attività dei dipendenti collegati in rete.

Indice

Capitolo 1

La prestazione lavorativa nell'evoluzione verso la knowledge economy

1.1 La teoria dell'impresa

Secondo il Codice Civile, l'impresa è "un'attività economica organizzata al fine della produzione o dello scambio di beni o di servizi", fornisce quindi prodotti e servizi, crea posti di lavoro, genera ricchezza sotto forma di profitti e li ridistribuisce attraverso i dividendi. Vi sono diverse problematiche da gestire per un'impresa, sia internamente, che esternamente: il comportamento dell'azienda deve allinearsi con quello di altri soggetti, come lo Stato, i consumatori e gli organismi internazionali; al suo interno si dovranno coordinare anche le diverse interazioni tra i soggetti che cooperano con l'impresa, dai dipendenti agli amministratori. L'imprenditore deve studiare al meglio le risorse che ha disposizione, per poter garantire un successo alla propria impresa, avendo come fine ultimo la creazione di valore economico. Il valore economico è inteso come un surplus di utilità per i soggetti che sono indispensabili per la sopravvivenza dell'impresa, che tendono quindi, a massimizzare

il proprio profitto[1]. L'impresa ha diverse risorse che interagiscono fra loro per raggiungere l'obbiettivo, che è la realizzazione del valore economico e vengono gestite attraverso l'organizzazione.

1.2 La teoria dell'organizzazione

Inizialmente, le prime teorie organizzative di inizio Novecento vedevano l'organizzazione come una macchina coordinata in maniera formale. I compiti, che venivano assegnati alle unità organizzative, erano molto formalizzati e basati su un sistema gerarchico: i dipendenti quindi, eseguivano le loro limitate attività come se fossero appunto delle macchine, in quanto si pensava che solo annullando gli aspetti relazionali della natura umana si potessero raggiungere appieno gli obbiettivi aziendali.
Successivamente, lo studioso Elton Mayo studiò il comportamento dei lavoratori, e mostrò che la produttività dei medesimi era influenzata positivamente anche dai fattori emotivi e relazionali, che sono requisiti fondamentali per creare una buona organizzazione. Queste teorie, le human relations theory (Mayo, 1933), sono alla base delle organizzazioni attuali e sono state create secondo una nuova concezione di razionalità: la razionalità limitata. Per razionalità limitata si intende la difficoltà che ha una persona a massimizzare il proprio valore economico, dovuto principalmente ai limiti del cervello umano nell'elaborazione delle informazioni e nella scelta ottimale di un'azione[2]. Il comportamento di un lavoratore non tende a massimizzare il proprio valore economico ma una propria utilità, che viene intesa come una propria soddisfazione personale e il livello di utilità che un dipendente ottiene dal proprio lavoro dipende quindi dalla soddisfazione dei propri bisogni personali.
Tutto ciò porta a pensare che l'organizzazione sarà molto più efficiente se si riuscirà ad unire il desiderio del lavoratore di massimizzare la propria utilità

[1] Agostino La Bella - Elisa Battistoni, *Economia e Organizzazione aziendale*, Apogeo, 2008

[2] Agostino La Bella - Elisa Battistoni, *Economia e Organizzazione aziendale*, Apogeo, 2008

con il desiderio dell'impresa di massimizzare il valore economico. Un esempio potrebbe essere un sistema organizzativo basato su una autonomia più accentuata del dipendente, che potrebbe aumentare lo sforzo creativo dello stesso e renderlo più propenso ad accettare le dinamiche e i cambiamenti organizzativi e permetterà, quindi, di massimizzare sia la soddisfazione personale del dipendente che il valore economico dell'impresa. Questo interesse per gli aspetti relazionali ed emozionali del dipendente ha portato all'identificazione di una nuova visione dell'organizzazione, che è avversa alla teoria meccanicistica delle prime teorie del Novecento e che ha portato alla creazione di nuovi modelli economici come la knowledge economy[3].

1.3 La knowledge economy

Nel taylorismo il controllo era il fondamento dell'impresa e creava una totale mancanza di attenzione per gli aspetti psicologici del lavoro.
Con l'evoluzione tecnologica, che si è creata negli ultimi anni, è nato un nuovo settore della scienza economica che calcola il valore dei fattori intangibili come l'educazione, la formazione e la comunicazione: si è creata quindi l'economia della conoscenza o knowledge economy.
Le imprese basate sulla knowledge economy sono imprese che non richiedono la precisione manageriale tipica del taylorismo, piuttosto la relazione, la capacità di connessione, di costruire reti di cooperazione tra i soggetti e che tiene conto delle nuove tecnologie di comunicazione, come i social network. Se l'economia industriale creava enormi concentrazioni di potere, l'economia della conoscenza le limita.
Questo nuovo modo di vedere l'economia è coerente con il mondo moderno, fatto di persone che si muovono costantemente, che creano delle comunità, dove la collaborazione risulta essere indispensabile[4].

[3]Agostino La Bella - Elisa Battistoni, *Economia e Organizzazione aziendale*, Apogeo, 2008

[4]Rossella Chiara Gambetti, *Le relazioni Internet-based nei mercati industriali*, Vita e Pensiero, 2005

Questo fenomeno globale è formato da tre principi:

1. Empowerment: è il processo di valorizzazione dei collaboratori che riduce il peso della gerarchia aziendale e premia il contributo di idee innovative del lavoratore;

2. Entrepreneurship: è l'insieme di abilità che consentono di individuare idee e aree di business;

3. Expertise: è una pratica basata sulla diagnosi che verte su una precisa padronanza delle conoscenze e delle abilità correlate ai compiti da svolgere.

Per comprendere al meglio la nascita e la sopravvivenza delle strategie di gestione delle risorse umane e di quanto sia in espansione la knowledge economy al giorno d'oggi, si può fare riferimento ad un modello agent-based per la simulazione di un mercato dove le imprese inviano le offerte di lavoro per riempire i posti vacanti e decidono come selezionare i dipendenti[5].
Il modello agent-based è strutturato in questo modo: le imprese selezionano i dipendenti in base alle loro competenze e gli esperimenti di simulazione indicano che, data una variazione dell'ambiente economico, l'occupazione a tempo indeterminato e la creazione di conoscenza specifica nei dipendenti sono una strategia di sopravvivenza per le imprese.
Lo studio presenta i risultati degli esperimenti attraverso il modello Firm-World, che contiene tre tipi di agenti: l'ambiente, le imprese e i dipendenti. Il modello contiene l'insieme di abilità dei dipendenti e le politiche di adattamento organizzativo dell'impresa, che attraverso il processo di selettiva assunzione dei dipendenti, potranno creare profitto per l'impresa o il suo fallimento. L'obiettivo degli esperimenti effettuati è quello di capire quale tipo di organizzazione può sopravvivere in un contesto economico odierno, in particolare, è interessante analizzare quale tipo di organizzazione è probabile

[5]per un'analisi completa della simulazione si veda, Edoardo Mollona - David Hales, *Knowledge-Based Jobs and the Boundaries of Firms Agent-based Simulation of Firms Learning and Workforce Skill Set Dynamics*, Springer, 2006

che emerga in un ambiente dinamico che cambia costantemente. Se si assume che nella knowledge economy, un numero crescente di discipline tecnologiche sono necessarie, e le organizzazioni hanno sempre più bisogno di contare su un gran numero di specialisti con delle conoscenze specifiche, allora è interessante osservare come le organizzazioni gestiscono il rapporto di lavoro con i loro dipendenti: dagli esperimenti effettuati si nota che le imprese avranno più possibilità di sopravvivenza in ambienti economici dinamici, quando usano contratti a tempo indeterminato per costruire e mantenere un repertorio di diverse abilità specifiche.
Questo studio suggerisce che nella knowledge economy è importante avere un numero crescente di specialisti in discipline tecnologiche. Si può notare che in ambienti dinamici le imprese che fanno affidamento su una disponibilità di specialisti diversi, riescono a gestire meglio i cambiamenti perché le competenze specifiche forniscono l'accesso a conoscenze all'avanguardia e soluzioni innovative che risolvono problemi organizzativi[6].
Nelle imprese che seguono la knowledge economy, quindi, non esiste più il concetto di "impero" formato da datori di lavoro inattaccabili e da lavoratori visti come semplici ingranaggi da far funzionare, non esiste più la modalità di relazione gerarchica, in quanto ormai è interattiva. Occorre però un accurato studio di leggi ad hoc, in quanto la necessità di controllare da parte del datore di lavoro queste relazioni tra lavoratori sembra essere motivata ai fini della prestazione lavorativa, ma potrebbe portare ad un abuso di potere.

[6]Edoardo Mollona - David Hales, *Knowledge-Based Jobs and the Boundaries of Firms Agent-based Simulation of Firms Learning and Workforce Skill Set Dynamics*, Springer, 2006

Capitolo 2

Il potere di controllo del datore di lavoro sui lavoratori

2.1 Il potere di controllo del datore di lavoro nel Codice Civile

La definizione di prestatore di lavoro contenuta nell'art. 2094 del codice civile afferma che: "E' prestatore di lavoro subordinato chi si obbliga mediante retribuzione a collaborare nell'impresa, prestando il proprio lavoro intellettuale o manuale alla dipendenza e sotto la direzione del datore di lavoro." L'articolo espone quindi le modalità secondo cui la prestazione lavorativa deve essere svolta, cioè il lavoratore dovrà collaborare con l'impresa sotto la direzione del datore di lavoro.
Il datore di lavoro ha il diritto di decisione sulla prestazione lavorativa nei limiti sanciti dall'art. 2013 del codice civile, il quale dispone: "Il prestatore di lavoro deve essere adibito alle mansioni per le quali è stato assunto o a quelle corrispondenti alla categoria superiore che abbia successivamente acquisito ovvero a mansioni equivalenti alle ultime effettivamente svolte, senza alcuna diminuzione della retribuzione. Nel caso di assegnazione a mansioni superiori il prestatore ha diritto al trattamento corrispondente all'attività svolta, e l'assegnazione stessa diviene definitiva, ove la medesima non abbia avuto

luogo per sostituzione di lavoratore assente con diritto alla conservazione del posto, dopo un periodo fissato dai contratti collettivi, e comunque non superiore a tre mesi. Egli non può essere trasferito da una unità produttiva ad un'altra se non per comprovate ragioni tecniche, organizzative e produttive. Ogni patto contrario è nullo."
Inoltre il datore di lavoro ha il diritto di esigere gli obbiettivi richiesti nella prestazione lavorativa e possiede anche il diritto di applicare sanzioni alle inosservanze del lavoratore. Questi diritti vengono descritti negli articoli 2104, 2105 e 2106 del codice civile. L'art. 2104 dichiara che: "Il prestatore di lavoro deve usare la diligenza richiesta dalla natura della prestazione dovuta, dall'interesse dell'impresa e da quello superiore della produzione nazionale. Deve inoltre osservare le disposizioni per l'esecuzione e per la disciplina del lavoro impartite dall'imprenditore e dai collaboratori di questo dai quali gerarchicamente dipende.".
L'art. 2105 sancisce che: "Il prestatore di lavoro non deve trattare affari, per conto proprio o di terzi, in concorrenza con l'imprenditore, né divulgare notizie attinenti all'organizzazione e ai metodi di produzione dell'impresa, o farne uso in modo da poter recare ad essa pregiudizio."
L'inadempienza del lavoratore ai sopraccitati articoli viene regolata dall'art. 2106 del codice civile: "L'inosservanza delle disposizioni contenute nei due articoli precedenti può dar luogo all'applicazione di sanzioni disciplinari, secondo la gravità dell'infrazione."
Questi articoli conferiscono quindi il potere di controllo al datore di lavoro sull'esecuzione della prestazione lavorativa da parte del lavoratore[1].

2.2 Il codice disciplinare aziendale

Il lavoratore, oltre a mancare nella prestazione lavorativa richiesta, potrebbe causare anche danni alla sicurezza informatica dell'azienda. I com-

[1]Franco Toffoletto, *Nuove tecnologie informatiche e tutela del lavoratore, il potere di controllo del datore di lavoro - il telelavoro*, Giuffrè editore, 2006

portamenti negativi, per essere contestati ed eventualmente sanzionati dal datore di lavoro, devono essere dichiarati e vietati al lavoratore nonché descritti nel codice disciplinare aziendale, che deve essere pubblicato mediante affissione in luogo pubblico dove tutti i lavoratori possano consultarlo[2]. Secondo l'art. 7 dello Statuto dei lavoratori: "Le norme disciplinari relative alle sanzioni, alle infrazioni in relazione alle quali ciascuna di esse può essere applicata ed alle procedure di contestazione delle stesse, devono essere portate a conoscenza dei lavoratori mediante affissione in luogo accessibile a tutti."

2.3 I controlli preventivi sulla prestazione lavorativa

Il primo comma dell'articolo 4 dello Statuto dei lavoratori, prevede un divieto assoluto ed inderogabile, sostenuto da sanzione penale, di installazione ed uso di impianti audiovisivi e di altre apparecchiature esclusivamente destinate al controllo dei lavoratori. Il secondo comma invece è un divieto flessibile, in quanto enuncia che i sistemi di controllo possono essere utilizzati, ma solo per quanto riguarda la sicurezza sul lavoro dell'azienda. Per l'istallazione di sistemi di controllo il datore di lavoro deve, inoltre, stabilire un accordo con la rappresentanza sindacale oppure ottenere il permesso della Direzione Provinciale del Lavoro.
Il problema dell'operatività dell'art. 4 nel nuovo contesto tecnologico è di estrema importanza: si ritiene da una parte che per la legislazione italiana gli strumenti che consentono il monitoraggio delle e-mail e degli accessi ad Internet facciano parte dei controlli a distanza e quindi rientrerebbero nell'applicabilità dell'art. 4, mentre dall'altra parte si reputa che l'art. 4 sia inapplicabile alla strumentazione informatica, per via della sua superficialità rispetto alla prestazione lavorativa. La giurisprudenza si dimostra particolar-

[2]Franco Toffoletto, *Nuove tecnologie informatiche e tutela del lavoratore, il potere di controllo del datore di lavoro - il telelavoro*, Giuffrè editore, 2006

mente aperta nel sancire la legittimità dei controlli difensivi, non sull'attività lavorativa, ma su possibili attività illecite del lavoratore[3].

2.4 Privacy: il controllo difensivo e il controllo occulto

Il controllo tecnologico può essere ritenuto legittimo solo se esso possa ritenersi indispensabile, in ogni caso, deve essere attuato in carattere difensivo preceduto da una adeguata informativa.
Quando il controllo occulto è permesso è applicabile l'art. 13, comma 5, lettera b, del Codice della privacy che esclude l'obbligo di informativa quando i dati servono per far valere un diritto in sede giudiziaria. Il controllo difensivo consiste in una forma di intervento, controllo o monitoraggio diretti ad accertare condotte illecite del lavoratore che integrino, appunto, lesione del patrimonio aziendale o della sicurezza o illecito contrattuale.[4].
L'art. 8 della Convenzione Europea sui diritti dell'uomo sancisce: "1. Ogni persona ha diritto al rispetto della sua vita privata e famigliare, del suo domicilio e della sua corrispondenza.
2. Non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura tale che in una società democratica, sia necessaria per la sicurezza nazionale, per la pubblica sicurezza, per il benessere economico del paese, per la difesa dell'ordine e per la prevenzione dei reati, per la protezione della salute o della morale o per la protezione dei diritti e delle libertà altrui.".
Un esempio di violazione dell'articolo 8 della Convenzione è avvenuto tra il 1998 e il 1999, quando la ricorrente Ms. Lynette Copland assistente di un università statale inglese, a sua insaputa, è stata sottoposta a controllo da

[3]Enrico Barraco - Andrea Sitzia, *La tutela della privacy nei rapporti di lavoro*, Ipsoa, 2008

[4]Enrico Barraco - Andrea Sitzia, *La tutela della privacy nei rapporti di lavoro*, Ipsoa, 2008

parte del suo dipartimento sulle modalità di utilizzo del telefono, posta elettronica e Internet.
Il controllo è avvenuto in particolare sulle fatture da cui si potevano ricavare i numeri di telefono, la durata e i costi delle comunicazioni effettuate, sui siti web visitati e sui tempi di connessione, e sulla posta elettronica per quanto riguarda gli indirizzi dei destinatari. La Corte Europea ha ritenuto il Regno Unito responsabile per la violazione dell'art. 8 della Convenzione. Secondo la Corte, anche le telefonate effettuate in ufficio rientrano nella nozione di "vita riservata" e di "corrispondenza" per gli scopi del par.1 di tale articolo. In tale ambito, devono essere considerate anche le e-mail trasmesse dall'ufficio e le informazioni derivate dal controllo dell'uso personale di Internet[5].

2.5 Il problema dei controlli sulla navigazione in Internet

Con l'avanzamento tecnologico degli ultimi decenni, sono sorti numerosi problemi sulla consultazione legislativa, in quanto vi è la mancanza di una normativa specifica. Lo Statuto dei lavoratori è stato elaborato in un tempo in cui il computer non era l'ordinario strumento di lavoro, quindi sarebbe necessario uno strumento legislativo in grado di tener conto di casistiche completamente nuove rispetto a quelle prese in considerazione quaranta anni orsono dal legislatore, il quale teneva conto di contesti tecnologici obsoleti rispetto agli attuali.
Quindi per quanto riguarda il controllo sui sistemi informatici si terrà presente l'applicazione di diversi apparati normativi. Internet ha raggiunto livelli così estesi nel campo lavorativo, da poter affermare che non esiste ormai alcuna azienda che ne precluda l'utilizzo. Il monitoraggio della navigazione in Internet da parte dei dipendenti è un problema per la legittimità del già citato potere di controllo del datore di lavoro; da una parte infatti vi sarà

[5]Enrico Barraco - Andrea Sitzia, *La tutela della privacy nei rapporti di lavoro*, Ipsoa, 2008

la necessità di evitare comportamenti illeciti da parte del lavoratore, come ad esempio navigare in siti potenzialmente pericolosi, rischiando di infettare con virus la rete aziendale, oppure scaricare video, programmi, software che non servano nell'ambito lavorativo e che potrebbero causare danni al sistema esponendo così l'azienda a costi considerevoli; dall'altra parte invece avremo il problema della liceità del controllo che può effettuare un datore di lavoro per scongiurare i problemi evidenziati in precedenza, onde evitare controlli invasivi, che comportino anche il trattamento dei dati sensibili come nel caso in cui ci sia un monitoraggio degli accessi a siti riguardanti l'orientamento politico, sindacale, religioso o anche sessuale del dipendente. Le linee guida sono dettate dal Garante per la protezione dei dati personali con deliberazione del 1° marzo 2007, n. 13[6].

2.5.1 Le linee guida del Garante della privacy sul monitoraggio informatico nel rapporto di lavoro

Il Garante nella deliberazione n.13 del 1° marzo 2007, indica ai datori di lavoro di provvedere all'affissione di un codice disciplinare aziendale, che dovrebbe specificare quale debba essere il corretto utilizzo di Internet, precisando i comportamenti illeciti, come il download di software (per esempio videogiochi), oppure file musicali o video.
Dovrebbe anche dichiarare se i dati vengono conservati e controllati dal datore di lavoro, se e in che modo si possa utilizzare la posta elettronica per ragioni personali specificando le modalità e gli orari in cui sia possibile farlo. Infine il datore di lavoro dovrebbe dichiarare le conseguenze risarcitorie e disciplinari in caso di un illecito utilizzo di Internet.
Il datore di lavoro ha il diritto di controllare la prestazione lavorativa ma è gravato dall'obbligo di informativa descritto nell'art. 13 del codice della privacy, su eventuali controlli interni. Il datore di lavoro però deve rispettare la libertà e la dignità del lavoratore, e sono vietate dall'art. 4 dello Statuto

[6]Enrico Barraco - Andrea Sitzia, *La tutela della privacy nei rapporti di lavoro*, Ipsoa, 2008

dei lavoratori le strumentazioni hardware e software finalizzate al monitoraggio della prestazione lavorativa, in quanto il trattamento dei dati che deriva dall'utilizzo dei succitati strumenti per il monitoraggio è illecito; e questo a prescindere dal fatto che il controllo sia occulto o meno[7].
Sono vietati infatti i software o hardware che consentono:

1. la lettura e la registrazione sistematica dei messaggi di posta elettronica;

2. la riproduzione ed eventuale memorizzazione delle pagine web che il lavoratore ha visualizzato;

3. la lettura e la registrazione dei caratteri inseriti tramite la tastiera o analogo dispositivo;

4. l'analisi occulta del personal computer del lavoratore.

Il Garante, per quanto riguarda la navigazione nel web, impone al datore di lavoro le seguenti disposizioni:
a) individuazione di categorie di siti considerati correlati o meno con la prestazione lavorativa;
In questo modo il lavoratore conoscerebbe anticipatamente quali siti web siano ritenuti collegati alla prestazione lavorativa e quali invece no. Questa misura è però difficilmente realizzabile per il fatto che ormai esistono milioni di siti web e ne nascono ogni giorno a migliaia. Il lavoratore, quindi, potrebbe trovarsi nella situazione in cui, per evitare di visitare un sito web che non faccia parte della lista dei siti navigabili e per timore di sanzioni, eviti di visitare anche siti che potrebbero essere rilevanti professionalmente.
b) configurazione di sistemi o utilizzo di filtri che prevengano determinate operazioni reputate non confacenti all'attività lavorativa, quali l'upload o l'accesso a determinati siti (inseriti in una sorta di blacklist) e/o il download di file o software aventi particolari caratteristiche (dimensionali o di tipologia

[7]Enrico Barraco - Andrea Sitzia, *La tutela della privacy nei rapporti di lavoro*, Ipsoa, 2008

di dati);

Questa seconda misura sembra essere più efficace di quella precedente, in quanto i software che bloccano l'accesso a determinati siti, creano un vero e proprio muro difensivo senza interferire con le normative sul controllo dei lavoratori.

c) trattamento di dati in forma anonima o tale da precludere l'immediata identificazione di utenti mediante loro opportune aggregazioni (ad es., con riguardo ai file di log riferiti al traffico web, su base collettiva o per gruppi sufficientemente ampi di lavoratori);

Il controllo anonimo può concludersi con un avviso generalizzato relativo ad un uso inconsueto degli strumenti aziendali. Il garante prescrive inoltre che in caso di assenza di successive anomalie non è di regola giustificato effettuare controlli su base individuale. Questa affermazione, però, è un mero indirizzo di massima, in quanto può verificarsi un controllo anche su una singola anomalia come, per esempio, nel caso in cui si sia infettato il sistema aziendale a causa di un virus letale, il datore di lavoro deve poter effettuare un controllo individuale, al fine di far valere le eventuali conseguenze sul piano risarcitorio, disciplinare e penale[8].

d) eventuale conservazione nel tempo dei dati strettamente limitata al perseguimento di finalità organizzative, produttive e di sicurezza.

I software devono essere quindi programmati per cancellare periodicamente i dati personali relativi agli accessi Internet, possono essere eventualmente prolungati i tempi di conservazione in casi eccezionali: esigenze tecniche e di sicurezza, indispensabilità del dato in sede giudiziaria, obbligo di consegnare i dati alle autorità giudiziarie.

2.5.2 La casistica giurisprudenziale

La giurisprudenza per quanto riguarda i controlli degli accessi ad Internet non offre ancora soluzioni sicure, in quanto non ci sono percorsi argomentativi

[8]Enrico Barraco - Andrea Sitzia, *La tutela della privacy nei rapporti di lavoro*, Ipsoa, 2008

consolidati. I giudici hanno un maggiore interesse in due nodi interpretativi: l'applicabilità dell'art. 4 dello Statuto dei lavoratori al monitoraggio degli accessi ad Internet e la liceità dei controlli difensivi[9].
La sentenza del Tribunale di Milano 8 giugno 2001 dichiara: "il comportamento del lavoratore, consistito in un collegamento quotidiano alla rete Internet per più ore al giorno in assenza di effettive necessità lavorative, costituisce un rilevante inadempimento degli obblighi di diligenza e integra una giusta causa di licenziamento; il datore di lavoro può fornire la prova dei collegamenti contestati, oltre che mediante testimoni, anche attraverso l'allegazione dei dati forniti dal provider circa gli accessi alla rete provenienti da ogni singola postazione di lavoro". Il lavoratore quindi è stato licenziato con giusta causa per l'inadempimento al proprio lavoro e l'impresa informatica ha provato tale inosservanza senza contravvenire l'art. 4, in quanto, non vi sono state violazioni della privacy, dato che il provider ha fornito solamente gli accessi dalle singole postazioni di lavoro[10].
Un altro caso importante riguarda una dipendente, che è stata incolpata di inadempienze lavorative e successivamente licenziata per i seguenti motivi: "sono emersi collegamenti Internet giornalieri di durata lunghissima, due da circa due ore ciascuno o uno solo da tre o quattro ore, se non di più, in coincidenza con la sua presenza al lavoro.".
L'istruttoria ha voluto accertare che le mansioni della dipendente richiedessero collegamenti limitati, che i collegamenti contestati fossero avvenuti effettivamente dal computer della dipendente, che la dipendente rimanesse connessa anche durante gli intervalli lavorativi, che ci fossero testimoni della sua inadempienza. Il tribunale ha convalidato l'esistenza della giusta causa di licenziamento, perché per diverse ore la lavoratrice non ha effettuato la prestazione per la quale era retribuita. Sono state sollevate numerose critiche verso la sentenza, in quanto non vi è stata una verifica sulla legittimità

[9]Enrico Barraco - Andrea Sitzia, *La tutela della privacy nei rapporti di lavoro*, Ipsoa, 2008

[10]Enrico Barraco - Andrea Sitzia, *La tutela della privacy nei rapporti di lavoro*, Ipsoa, 2008

del controllo tecnico e nessun accertamento sulla violazione dell'art. 4 dello Statuto dei lavoratori.
Si è ritenuto che questa sentenza segua le orme della dottrina minoritaria, che ritiene che i controlli tecnologici possano avvenire aggirando le rigide maglie statutarie. Secondo questa dottrina quindi "se il controllo non comprende, in senso complessivo, l'attività del lavoratore, ma si limiti alla verifica del corretto utilizzo degli strumenti messi a disposizione del datore di lavoro, detto controllo non rientra, non solo nella fattispecie di cui all'art. 4, comma 1, ma nemmeno in quella in cui all'art. 4, comma 2[11].
Negli ultimi tempi sembra prevalere però la giurisprudenza più rigorosa e meno liberale, che tende a privilegiare in modo più severo le istanze di libertà e dignità dei lavoratori. Si può citare, quindi, la sentenza del Tribunale di Milano 31 marzo 2004, dove era stato preso in esame il licenziamento di una lavoratrice che aveva usufruito del servizio Internet per scopi non lavorativi, con violazione della policy interna che vietava ai dipendenti "l'accesso a detti sistemi e tantomeno all'utilizzo dei medesimi per fini diversi."
La datrice di lavoro si era servita delle rilevazioni di un programma di controllo chiamato Super Scout, che acquisiva automaticamente tutte le informazioni sugli accessi ad Internet, la durata, la frequenza dei collegamenti effettuati tenendo in memoria gli ultimi due mesi di navigazione; i tabulati venivano successivamente consegnati al direttore del personale.
Il Tribunale di Milano ha concluso che l'utilizzo di software in grado di memorizzare automaticamente tutte le navigazioni in Internet dei dipendenti e quindi di riconoscere e verificare chi adempie o meno alla prestazione lavorativa integra la condotta vietata dell'art. 4, comma 2 dello Statuto dei lavoratori e che il monitoraggio degli accessi ad Internet e la conservazione dei dati può rientrare nella violazione del Codice della privacy sul trattamento dei dati sensibili. Infatti, dai dati memorizzati dal software, si possono ricavare opinioni politiche, religiose o sindacali del singolo dipendente violan-

[11] Enrico Barraco - Andrea Sitzia, *La tutela della privacy nei rapporti di lavoro*, Ipsoa, 2008

do anche l'art. 8 dello Statuto dei lavoratori che limita il diritto di indagine del datore di lavoro sui propri dipendenti. La Corte di Appello di Milano, 30 settembre 2005, dichiara: "i programmi informatici che consentono il monitoraggio della posta elettronica e degli accessi ad Internet sono necessariamente delle apparecchiature di controllo nel momento in cui, in ragione delle loro caratteristiche, consentono al datore di lavoro di controllare a distanza e in via continuativa durante la prestazione l'attività lavorativa e se la stessa sia svolta in termini di diligenza e di corretto adempimento".
Secondo il Garante della privacy se la finalità è quella di dimostrare una condotta illecita del lavoratore, consistita nell'utilizzo indebito di Internet, il datore di lavoro dovrebbe limitarsi a provare l'illecita navigazione in rete e i relativi tempi di collegamento rispettando il principio di pertinenza e non eccedenza descritto nell'art. 11 del Codice della privacy (par.6): il datore di lavoro deve infatti trattare i dati nella misura meno invasiva possibile.[12]
Per quanto riguarda i controlli difensivi, da un lato vi sarà l'obbligo di effettuare i dovuti controlli al sistema informatico aziendale da parte del datore di lavoro, e dall'altro lo stesso non potrà usare i risultati di questi controlli contro eventuali condotte illecite dei dipendenti per il limite imposto dall'art. 4 dello Statuto dei lavoratori. Non sarà sufficiente invocare la necessità di preservare la sicurezza del sistema informatico aziendale, ma sarà necessario che il controllo sia effettuato per la tutela del patrimonio aziendale contro atti illeciti dei propri dipendenti e che la vigilanza sia mantenuta in una dimensione umana e senza l'uso di tecnologie che la rendono continua e anelastica. Per i possibili danni arrecati da virus informatici, il datore di lavoro potrà sanzionare il dipendente che ha causato il danno, ma non potrà contestare al lavoratore il tempo impiegato per i collegamenti che hanno portato all'infezione: bisognerebbe infatti, dare la possibilità al datore di lavoro di poter esaminare ogni sito visitato dal dipendente per accertare se il virus sia stato contratto in maniera incolpevole, utilizzando così i dati sensibili del

[12]Enrico Barraco - Andrea Sitzia, *La tutela della privacy nei rapporti di lavoro*, Ipsoa, 2008

lavoratore[13].

2.6 I controlli sulla posta elettronica e i controlli sulla memoria di massa

Un altro importante problema riguarda le modalità di utilizzo del computer da parte del lavoratore e i possibili controlli da parte del datore di lavoro per quanto riguarda la posta elettronica. Senza la previa autorizzazione da parte del datore di lavoro per un uso privato dello strumento, il dipendente non potrà utilizzare il computer per fini personali come conservare foto, documenti o utilizzare software non aziendali.
Quando il datore di lavoro controllerà la memoria di massa del server o del computer vi sarà il problema di tracciare il limite di liceità sul controllo dei propri dipendenti. Per valutare i problemi connessi con l'utilizzo della posta elettronica, si può analizzare in primo luogo l'art. 15 della Costituzione che sancisce: "La libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione sono inviolabili. La loro limitazione può avvenire soltanto per atto motivato dell'autorità giudiziaria con le garanzie stabilite dalla legge."; per corrispondenza si intende lo scambio di informazioni e messaggi fra persone e più precisamente ne spiega il significato l'art. 616 ultimo comma, del Codice Penale: "Agli effetti delle disposizioni di questa sezione, per "corrispondenza" si intende quella epistolare, telegrafica, telefonica, informatica o telematica ovvero effettuata con ogni altra forma di comunicazione a distanza.".
Vi sono conseguenze diverse nel caso in cui la corrispondenza sia "aperta" o "chiusa": nel caso della posta elettronica possiamo affermare che si tratti di una corrispondenza "aperta" in quanto sulla rete il messaggio è conoscibile da terzi e si può paragonare a una cartolina, per la quale, in quanto aperta, non è possibile pretendere la riservatezza della medesima. L'eventuale password

[13]Enrico Barraco - Andrea Sitzia, *La tutela della privacy nei rapporti di lavoro*, Ipsoa, 2008

nella posta elettronica, porterebbe la corrispondenza ad essere classificata come "chiusa" e rientrerebbe nella tutela prevista dal citato art. 616 del codice penale[14].
Dopo aver analizzato l'articolo in questione sembra che il datore di lavoro non commetta reato nel caso di controllo della posta elettronica "aperta", ma vi sono altre normative che possono essere violate. E' necessario innanzitutto esaminare le linee guida del Garante della privacy nella deliberazione del 1° marzo 2007, n.13.

2.6.1 Le linee guida del Garante della privacy sull'utilizzo della posta elettronica

I messaggi di posta elettronica, come citato in precedenza, sono forme di corrispondenza sostenute da garanzie di segretezza tutelate costituzionalmente.
Secondo il Garante: "La mancata esplicitazione di una policy al riguardo può determinare anche una legittima aspettativa del lavoratore, o di terzi, di confidenzialità rispetto ad alcune forme di comunicazione. Tali incertezze si rispecchiano sulla qualificazione, in termini di liceità, del comportamento del datore di lavoro che intenda apprendere il contenuto di messaggi inviati all'indirizzo di posta elettronica usato dal lavoratore (posta in entrata) o di quelli inviati da quest'ultimo (posta in uscita)."
Vengono successivamente stabilite le seguenti linee guida:
a) il datore di lavoro deve rendere disponibili indirizzi di posta elettronica condivisi tra più lavoratori (ad esempio, info@ente.it, ufficiovendite@ente.it, ufficioreclami@società.com, urp@ente.it, etc.), eventualmente affiancandoli a quelli individuali (ad esempio, m.rossi@ente.it, rossi@società.com, mario.rossi@società.it);
Con questo accorgimento si evitano problemi legati all'assenza dei lavoratori, e la rotazione dei lavoratori sull'utilizzo di quella determinata casella di posta

[14]Franco Toffoletto, *Nuove tecnologie informatiche e tutela del lavoratore, il potere di controllo del datore di lavoro - il telelavoro*, Giuffrè editore, 2006

elettronica evita il controllo individuale.

b) il datore di lavoro valuti la possibilità di attribuire al lavoratore un diverso indirizzo destinato ad uso privato del lavoratore;

Il Garante indica l'utilizzo di una posta elettronica per un uso privato dello strumento, ma nel momento in cui viene dato in uso un indirizzo privato con cui il lavoratore può inviare e-mail, si può creare il dubbio sul tempo che viene sottratto all'attività lavorativa.

c) il datore di lavoro metta a disposizione di ciascun lavoratore apposite funzionalità di sistema, di agevole utilizzo, che consentano di inviare automaticamente, in caso di assenze (ad es., per ferie o attività di lavoro fuori sede), messaggi di risposta contenenti le "coordinate" (anche elettroniche o telefoniche) di un altro soggetto o altre utili modalità di contatto della struttura. E' parimenti opportuno prescrivere ai lavoratori di avvalersi di tali modalità, prevenendo così l'apertura della posta elettronica.

In caso di eventuali assenze non programmate (ad es., per malattia), qualora il lavoratore non possa attivare la procedura descritta (anche avvalendosi di servizi webmail), il titolare del trattamento, perdurando l'assenza oltre un determinato limite temporale, potrebbe disporre lecitamente, sempre che sia necessario e mediante personale appositamente incaricato (ad es., l'amministratore di sistema oppure, se presente, un incaricato aziendale per la protezione dei dati), l'attivazione di un analogo accorgimento, avvertendo gli interessati;

Questa disposizione appare condivisibile per la protezione della privacy del lavoratore assente e si elimina la necessità del datore di lavoro o di altri colleghi di dover aprire e-mail destinate al medesimo. Nel caso in cui per esigenze lavorative si debba conoscere il contenuto della e-mail, l'interessato deve delegare un altro lavoratore chiamato "fiduciario", che ne controlli il contenuto, e informare il dipendente assente del controllo effettuato.

Si può però creare il problema del potere che viene devoluto al fiduciario, che è superiore anche a quello del datore di lavoro che può solo conoscere il contenuto della e-mail, ma non può aprirla. Ecco un esempio del problema

che si potrebbe creare: se il lavoratore fosse assente per malattia e il giorno stesso lo comunicasse all'azienda, ipotizzando che il fiduciario sia in trasferta e vi rimanga per un prolungato periodo di tempo, e proprio in quel momento dovesse arrivare un'e-mail molto importante ai fini aziendali, secondo questa disposizione, per rispettare la libertà del lavoratore, il datore di lavoro dovrebbe aspettare per prendere visione dell'e-mail, fino al rientro di uno dei due dipendenti? La risposta sembra essere ragionevolmente negativa[15].
d) in previsione della possibilità che, in caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa, si debba conoscere il contenuto dei messaggi di posta elettronica, l'interessato sarà messo in grado di delegare un altro lavoratore (fiduciario) a verificare il contenuto di messaggi e a inoltrare al titolare del trattamento quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. A cura del titolare del trattamento, di tale attività dovrebbe essere redatto apposito verbale e informato il lavoratore interessato alla prima occasione utile;
Per ovviare al problema precedente, viene descritta questa interessante e utile disposizione che permette al datore di lavoro di poter leggere le e-mail, in quanto sono di natura professionale e non private.
Ed infine,
e) i messaggi di posta elettronica contengano un avvertimento ai destinatari in cui sia dichiarata l'eventuale natura non personale dei messaggi stessi, precisando se le risposte possano essere conosciute nell'organizzazione di appartenenza del mittente e con eventuale rinvio alla predetta policy datoriale.

2.6.2 La casistica giurisprudenziale

A fronte di una condotta lesiva della libertà e segretezza della corrispondenza vi sono gli art. 616 -618 del codice penale; l'art. 616 dichiara che chiunque prenda cognizione del contenuto di una corrispondenza chiusa, a

[15]Enrico Barraco - Andrea Sitzia, *La tutela della privacy nei rapporti di lavoro*, Ipsoa, 2008

lui non diretta, ovvero sottrae o distrae, al fine di prendere o di farne da altri prendere cognizione, una corrispondenza chiusa o aperta, a lui non diretta, ovvero, in tutto o in parte, la distrugge o sopprime, è punibile con una sanzione. Emerge quindi l'interesse del datore di lavoro di conoscere in che modo poter effettuare controlli senza ricadere nel reato di violazione della corrispondenza.

Un datore di lavoro è stato accusato di violazione della corrispondenza di cui l'art. 616 c.p. in quanto l'imputato aveva preso visione della casella di posta del dipendente, e l'e-mail in particolare era rivolta ad un altro dirigente della stessa azienda. Il dipendente, è stato successivamente licenziato per aver inviato messaggi di posta elettronica contenenti dati riservati di carattere strategico relativi alla politica commerciale ed ai prezzi del proprio settore. In questa società vi era una policy aziendale in cui si precisava che "la strumentazione informatica è di proprietà aziendale in quanto mezzo di lavoro, è pertanto fatto divieto di utilizzo del mezzo informatico e delle trasmissioni interne ed esterne con esso effettuate per fini ed interessi non strettamente coincidenti con quelli della società...", "ogni computer deve essere protetto da password". Il Supremo Collegio ha ritenuto che la sentenza non potesse che essere assolutoria perché il fatto non sussisteva. Si è ritenuto altresì, che la corrispondenza informatica potesse essere qualificata chiusa solo nei confronti dei soggetti che non fossero stati legittimati all'accesso ai sistemi informatici di invio e ricezione dei singoli messaggi, ma in quanto il sistema è protetto da password, deve ritenersi che la corrispondenza possa essere conoscibile lecitamente solo da chi possiede la chiave informatica di accesso. Il collegio cita anche il provvedimento del Garante n.13 del 1° marzo 2007 " i dirigenti dell'azienda accedono legittimamente ai computer in dotazione ai propri dipendenti, quando delle condizioni di tale accesso sia stata loro data piena informazione".

E' interessante capire anche se sia applicabile o meno l'art. 4 dello Statuto dei lavoratori, e la Corte di Appello di Milano 30 settembre 2005 dichiara: "i programmi informatici che consentono il monitoraggio della posta elettroni-

ca e degli accessi ad Internet sono necessariamente delle apparecchiature di controllo nel momento in cui, in ragione delle loro caratteristiche, consentono al datore di lavoro di controllare a distanza e in via continuativa l'attività lavorativa; malgrado la natura di controllo a distanza non si ricade nell'ipotesi del divieto assoluto ed inderogabile di cui al primo comma dell'art. 4 dello Statuto dei lavoratori in quanto appare meritevole di tutela la finalità di proteggere da aggressioni informatiche esterne il sistema informatico aziendale, con possibile necessità di monitorare gli accessi verso l'esterno.", tutto ciò ad avviso della Corte è necessario e sufficiente per legittimare l'applicazione del comma 2 dell'art. 4 dello Statuto dei lavoratori[16].
Il datore di lavoro può effettuare controlli di tipo difensivo e, se nell'effettuazione di un controllo obbligato per la sicurezza aziendale riscontrasse condotte illecite, vi è la possibilità di sanzionarle. L'adozione di una adeguata policy interna è molto importante, in quanto se le norme aziendali prevedono che l'utilizzo di un determinato indirizzo di posta elettronica sia esteso ad una schiera di soggetti più ampia del solo lavoratore assegnatario dell'indirizzo stesso, non sarà necessaria l'apertura dei messaggi inviati e ricevuti attraverso quell'indirizzo da parte del datore di lavoro.

2.7 La videosorveglianza

La videosorveglianza ha un divieto assoluto per quanto riguarda il controllo diretto sull'adempimento lavorativo del dipendente, e un divieto flessibile per il caso in cui la sorveglianza sia richiesta da particolari esigenze aziendali e di sicurezza e comporti in via indiretta la possibilità di controllo a distanza dell'attività dei lavoratori (quando il datore di lavoro abbia installato apparecchiature senza rispettare l'art. 4, comma 1, dello Statuto dei lavoratori "E' vietato l'uso di impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori.").

[16]Enrico Barraco - Andrea Sitzia, *La tutela della privacy nei rapporti di lavoro*, Ipsoa, 2008

Nell'esempio formulato dal Garante nel provvedimento del 29 aprile 2004, nel caso dell'autobus si può pensare ad una compagnia di trasporto, che installi videocamere per controllare condotte illecite dei passeggeri sui propri mezzi. Questo tipo di controllo, è un controllo difensivo rivolto alla sicurezza, ma nel caso in cui si rilevino inadempienze da parte del conducente, la compagnia può prendere provvedimenti in base ai video registrati? La risposta del Garante è l'impossibilità di utilizzare le immagini ai fini indicati per il caso in cui l'azienda non avesse rispettato l'art. 4 dello Statuto dei lavoratori, comma 2, "la generica esigenza difensiva, di per sé, come detto sopra con riferimento ai controlli informatici, pur essendo necessaria non è da sola sufficiente ad immunizzare il controllo datoriale dalle rigide pastoie dello Statuto[17].".

2.8 Il potere di controllo in casi particolari

Normalmente il potere di controllo fino ad ora è stato esaminato solo nell'ambito del rapporto di lavoro subordinato. Per lo svolgimento della propria attività il datore di lavoro oltre che ai propri lavoratori si affida anche a collaboratori. Sono soggetti che collaborano con il datore di lavoro, ma non sono sottoposti al potere di controllo del medesimo. Un esempio potrebbe essere il lavoratore a progetto, che gestisce autonomamente l'esecuzione della prestazione ma che effettua una coordinazione con l'organizzazione del committente.

Come viene gestito il potere di controllo sul collaboratore? Come nel lavoro subordinato vi potrà essere il controllo sull'esatto adempimento del contratto, ma non potrà essere poi utilizzato al fine di esercitare il potere disciplinare, come avviene nel lavoro subordinato, cioè non potrà avere ad oggetto lo svolgimento dell'attività lavorativa nel tempo, ma avrà per oggetto l'opera o il servizio. Il committente, a differenza del lavoratore subordinato non gode delle garanzie dello Statuto dei lavoratori, come per esempio l'art. 2,3,4 e 5.

[17]Franco Toffoletto, *Nuove tecnologie informatiche e tutela del lavoratore, il potere di controllo del datore di lavoro - il telelavoro*, Giuffrè editore, 2006

Il committente potrebbe utilizzare telecamere o altri strumenti per controllare l'attività dei collaboratori con i soli limiti di garanzia, per il collaboratore, imposti dalla legge sulla protezione dei dati personali[18].

[18]Franco Toffoletto, *Nuove tecnologie informatiche e tutela del lavoratore, il potere di controllo del datore di lavoro - il telelavoro*, Giuffrè editore, 2006

Capitolo 3

L'effetto di Internet sui costi di transazione e sui costi opportunità

In questo capitolo ci si soffermerà sull'aspetto economico e sui mancati guadagni che si possono verificare durante una transazione o un rapporto di lavoro, in particolare si analizzeranno le variazioni dei medesimi a causa dell'utilizzo di Internet in un'impresa.

3.1 I costi di transazione

Si ha una transazione quando vi è uno scambio di beni o servizi: questo scambio genera diversi costi, tra i quali quelli di transazione. Questi costi non comprendono il costo dell'oggetto scambiato, ma sono relativi ai costi opportunità generati da una mancata transazione. Una mancata transazione si può verificare, per esempio, quando il contatto tra compratore e venditore è imperfetto e quindi alcune transazioni potenzialmente vantaggiose rimarranno opportunità non sfruttate. Dei costi di transazione fanno parte anche i costi opportunità, ossia, quando si opta per una scelta, vi saranno costi opportunità su quello a cui si è rinunciato, optando per quella scelta invece

di un'altra. I costi opportunità saranno descritti ed analizzati maggiormente in seguito. Un esempio di costo di transazione può essere una transazione via Internet tra due soggetti, uno dei quali sarà più diffidente sul completare o meno lo scambio, dovrà quindi sostenere molti costi di transazione per assicurarsi che l'altra parte tenga fede al contratto, e vi saranno anche costi opportunità per aver scelto quel soggetto piuttosto che un altro.
E' necessario cercare di delineare l'influenza che è in grado di esercitare Internet sui costi di transazione e sull'interazione sociale: per quanto riguarda i cosi di transazione, Internet consente di ridurli in modo considerevole.
I costi di transazione si dividono in costi di coordinamento e costi di incentivazione: i costi di coordinamento sono i costi per il tempo speso da parte dei consumatori per ricercare un prodotto, per determinarne il prezzo, o per stabilirne la qualità, per i produttori invece i costi di coordinamento riguardano le ricerche di mercato o le spese pubblicitarie per far conoscere il prodotto. Internet consente di ridurre i costi di ricerca, attraverso la riduzione del tempo e degli sforzi per individuare sia i prodotti, che i fornitori ed i clienti. Per l'individuazione dei prodotti, che rispondono ai bisogni dei soggetti coinvolti nello scambio, verranno utilizzati per esempio dei motori di ricerca. Per quanto riguarda i fornitori e i clienti, si ricorrerà ad esempio a marketplace digitali che sono una piattaforma virtuale, all'interno della quale avvengono transazioni commerciali che uniscono online fornitori e acquirenti[1].
I costi d'incentivazione si riferiscono ai costi di un determinato comportamento opportunistico e ai costi per prevenirlo. I costi d'incentivazione possono nascere da asimmetrie informative, ovvero dalla mancanza di informazioni utili, per prendere una decisione, e dall'imperfetta capacità di tenere fede agli impegni, vale a dire l'impossibilità delle parti di vincolarsi a mantenere promesse o le minacce fatte prima del raggiungimento di un accordo[2]. Internet, permette di ridurre tali costi, in quanto offre la possibilità per i soggetti

[1] Rossella Chiara Gambetti, *Le relazioni Internet-based nei mercati industriali*, Vita e Pensiero, 2005

[2] Agostino La Bella - Elisa Battistoni, *Economia e Organizzazione aziendale*, Apogeo, 2008

dello scambio di emettere e ricevere ordini, fatture, pagamenti online, che consentono rapide e complete procedure di controllo. In più, l'attività di chat line, newsgroup, forum e social network forniscono in modo continuativo soluzioni ad eventuali problemi relativi ai fornitori o ai prodotti. Inoltre, Internet consente di ridurre le asimmetrie informative e i costi d'intermediazione delle parti per esempio con la visione diretta dei prodotti online e delle condizioni contrattuali[3].

3.1.1 Le principali cause dei costi di transazione

I principali aspetti che influenzano i costi di transazione sono:

- *la specificità degli investimenti richiesti per condurre la transazione;*
  Durante la transazione si potrebbe dover effettuare alcuni investimenti specifici: se un produttore investe sui macchinari per la produzione di un determinato detersivo e li utilizza per soddisfare molti clienti, non ci sono investimenti specifici da effettuare; se invece un subappaltatore fabbrica componenti per l'Airbus 380, dovrà effettuare investimenti specifici per questa produzione e, a meno che non si sia stipulato un contratto definitivo con il cliente, non correrà il rischio in un investimento. La specificità degli investimenti rende le parti timorose di sottoscrivere un impegno, che potrebbe essere insoddisfacente.

- *la complessità della transazione e l'incertezza sulla prestazione;*
  Partendo dal concetto di razionalità limitata, le parti prenderanno accordi senza aver considerato ogni eventualità. In ogni transazione c'è un grado di complessità e di incertezza che porta costi di transazione alle parti, l'incertezza su diversi eventi che possono emergere durante il contratto o la complessità del compito rendono ardua la determinazione di possibili soluzioni per ogni evenienza.

[3]Rossella Chiara Gambetti, *Le relazioni Internet-based nei mercati industriali*, Vita e Pensiero, 2005

- *la frequenza con cui si verificano transazioni, e il periodo di tempo in cui si ripetono;*
  Se le transazioni vengono effettuate ripetutamente nel tempo, i soggetti riusciranno ad individuare comportamenti di routine che abbasseranno i costi di transazione, al contrario, nel caso di transazioni rare o uniche, le parti dedicheranno molto tempo allo studio del singolo scambio aumentando i costi di transazione.

- *la difficoltà di misurazione dei benefici della prestazione;*
  E' probabile che in una contrattazione con degli aspetti ambigui, una delle due parti si impegnerà maggiormente per verificare che la prestazione dell'altra parte sia conforme a quanto promesso nel contratto.

- *relazione con le altre transazioni;*
  Con l'aumentare del collegamento e della connessione delle transazioni, il costo per valutarle e farle rispettare aumenta notevolmente e i costi aumentano anche al crescere delle persone coinvolte[4].

3.1.2 Minimizzare i costi di transazione: l'integrazione verticale e Internet

I costi di transazione influenzano le scelte delle imprese, come la decisione di svolgere in proprio un'attività o di affidarla all'esterno. I costi e i profitti, che possono derivare dall'utilizzo del mercato, si possono classificare in base all'efficienza tecnica o all'efficienza di agenzia: l'efficienza tecnica indica se l'impresa sta utilizzando o meno il processo produttivo meno costoso, mentre l'efficienza di agenzia indica se l'impresa sta minimizzando i costi di coordinamento nello scambio di beni e servizi. L'interazione tra efficienza tecnica ed efficienza di agenzia comporta la scelta tra integrazione verticale e con-

[4] Agostino La Bella - Elisa Battistoni, *Economia e Organizzazione aziendale*, Apogeo, 2008

trattazioni di mercato[5].
Il mercato tende a minimizzare i costi di produzione, mentre l'integrazione verticale minimizza i costi di transazione: se l'impresa decidesse di accrescere la produzione al proprio interno invece di affidarsi al mercato, potrebbe sfruttare le economie di scala, ovvero potrebbe creare valore economico grazie all'incremento della dimensione della capacità produttiva.
Per evitare un ulteriore aumento di costi di transazione, sarebbe opportuno evitare un elevato grado di specificità dell'attività, per esempio, quando uno o più soggetti devono sostenere costi più o meno rilevanti per cambiare interlocutore. Questa situazione, può avvenire nel caso in cui un'impresa può scegliere fra molti possibili partner e una volta concluso il contratto con uno di essi non potrà più optare per altri collaboratori. In assenza di questa specificità non vi sarebbe alcun vincolo all'interruzione della relazione e ciascun soggetto potrebbe rimettersi sul mercato con altri soggetti[6].
Come è stato detto precedentemente, per minimizzare i costi di transazione è preferibile integrare verticalmente l'impresa. L'integrazione verticale significa estendere le attività dell'impresa a valle, verso i mercati finali dei prodotti, o a monte, quando l'impresa vuole assicurarsi fonti di approvvigionamento, diminuendo i relativi costi e garantendo al ciclo di produzione una certa continuità, e verranno introdotte produzioni in precedenza acquistate all'esterno. Quindi, l'obbiettivo può essere la riduzione dell'incertezza legata all'approvvigionamento dei fattori produttivi, oppure il raggiungimento della stabilità dei flussi di vendita[7].
La decisione, oltre a includere la convenienza economica, dipende anche dalla dimensione dell'impresa, infatti, le imprese innovative integreranno al loro interno tutte le attività e i servizi necessari alla produzione di beni, mentre le imprese, che possono contare su rapporti di lunga durata con i fornitori

[5]Agostino La Bella - Elisa Battistoni, *Economia e Organizzazione aziendale*, Apogeo, 2008
[6]Susanna di Martino - Cinzia Parolini, *Scelte di economia aziendale*, Il Mulino, 1998
[7]Agostino La Bella - Elisa Battistoni, *Economia e Organizzazione aziendale*, Apogeo, 2008

esterni, si serviranno del mercato.
Attualmente vi sono dibattiti fra i ricercatori per stabilire se l'utilizzo di Internet da parte di un'impresa possa influenzare le scelte di integrazione verticale, favorendo l'esternalizzazione di fasi di processi di sviluppo e di produzione di beni e servizi. Da una parte vi saranno dei costi di gestione delle informazioni molto ridotti, che garantiscono il coordinamento fra soggetti e favoriscono l'esternalizzazione dei processi produttivi, grazie alla riduzione dei costi di ricerca di fornitori che Internet garantisce. Dall'altra parte, invece, si afferma che Internet consente anche una più stretta integrazione tra i soggetti di una stessa impresa, che può essere gestita attraverso la gerarchia anziché dal mercato, attraverso per esempio una rete Extranet, che connette tra loro più reti locali, creando un network di aziende diverse. Soci, fornitori, dipendenti accedono alle medesime informazioni, utilizzando una rete protetta[8].

3.2 I costi opportunità

Il costo totale di tutto quello che acquistiamo comprende anche tutto ciò a cui dobbiamo rinunciare intraprendendo quell'azione: possiamo quindi parlare di costo opportunità, perché rinunciamo all'opportunità di avere qualcos'altro che gradiamo. Un costo opportunità può crearsi, per esempio, quando un datore di lavoro utilizza dei blocchi per quanto riguarda la navigazione nel web, evitando dei siti che potrebbero essere utili per l'attività lavorativa e perdendo quindi un possibile guadagno.
Ogni azione che si compie utilizza una certa quantità di tempo o di denaro, questo tempo e questo denaro si sarebbero potuti utilizzare per compiere un'altra azione, generando così costi opportunità. Il costo opportunità di una scelta è costituito dalla migliore di tutte le possibili alternative a tale scelta[9].

[8]Rossella Chiara Gambetti, *Le relazioni Internet-based nei mercati industriali*, Vita e Pensiero, 2005

[9]Marc Lieberman - Robert Hall, *Principi di economia*, Apogeo, 2006

La maggior parte delle volte il costo opportunità è quantificato in denaro, per esempio, se si acquistasse un televisore a duecento euro, si potrebbe pensare ad un altro prodotto, che si sarebbe potuto acquistare con la stessa somma di denaro. Altre volte invece il costo opportunità è quantificato in tempo: per esempio, se si decidesse di andare a fare una passeggiata, sarebbe implicata solo la perdita di tempo e non di denaro, anche se gli economisti attribuiscono un valore monetario approssimato anche nel caso di azioni che non portano a movimenti monetari.
Verrà analizzato ora il caso precedentemente descritto: un lavoratore ha un determinato compito ma è limitato dai blocchi imposti dal datore di lavoro. Si supponga che il datore di lavoro dia il compito ad un dipendente di acquistare una nuova fotocopiatrice professionale per una piccola azienda di pochi dipendenti, ordinandola via Internet: si analizzeranno ora, le possibili soluzioni che il datore di lavoro avrebbe a disposizione sapendo, che vi saranno costi opportunità espliciti, ovvero il denaro cui si rinuncia effettuando un pagamento quando si compie una scelta, oppure opportunità implicite, ovvero il valore di ciò che si sacrifica senza effettuare pagamenti in denaro come, per esempio, il tempo perso.
La nuova fotocopiatrice da acquistare viene cercata nei siti Internet di vari negozi, ma i limiti imposti dal datore di lavoro nella blacklist, impediscono di visualizzare alcuni siti con una promozione per quel prodotto. Il dipendente ordina quindi la fotocopiatrice pagandola 2500 euro senza trasporto in azienda, mentre se avesse usufruito della promozione il prezzo sarebbe stato di 2300 euro con trasporto gratis in azienda. Il datore di lavoro, ignaro di questa promozione, decide di risparmiare evitando di chiamare un'impresa di trasporti e assegna il compito di ritirare la fotocopiatrice al dipendente che ha effettuato l'ordine e ad altri due suoi colleghi; il prezzo totale sarà 20 euro di benzina.
I costi opportunità espliciti sono i 200 euro di differenza e i 20 euro di benzina, ma vi sono anche i costi impliciti da prendere in considerazione. Il maggior sacrificio che rientra in questi costi è il tempo, ma come si può calcolare il

valore del tempo? Dipende da cosa avrebbero fatto i dipendenti, se invece di perdere tempo nel trasporto avessero usufruito della promozione e quindi fossero rimasti in azienda ad aspettare la consegna gratuita. Gli economisti utilizzano un semplice metodo per calcolare il valore del tempo, ossia ogni ora utilizzata per la scelta compiuta va moltiplicata per il compenso orario della persona. Supponiamo che tutti e tre i dipendenti abbiano una retribuzione di 9 euro all'ora: per il trasporto della fotocopiatrice hanno impiegato 2 ore, quindi, in totale 54 euro.

Il datore di lavoro avrà perciò un costo opportunità totale per la scelta intrapresa di 274 euro, che sarà compensata da una parte dalla scelta di filtrare siti potenzialmente pericolosi e quindi di garantire la sicurezza aziendale ma dall'altra vi sarà una possibile perdita in denaro per aver impedito al lavoratore di utilizzare appieno gli strumenti messi a disposizione e, come in questo esempio, di aver optato per una scelta più dispendiosa.

Capitolo 4

La tutela dei diritti del lavoratore

4.1 I diritti del lavoratore: Costituzione e Statuto dei lavoratori

Nel secondo capitolo è stato approfondito il concetto di potere di controllo del datore di lavoro e come esso possa essere utilizzato sui dipendenti.
In questo capitolo ci si soffermerà sui diritti garantiti al lavoratore e sui limiti che impongono la Costituzione e lo Statuto dei lavoratori. La Costituzione fissa i primi limiti sui poteri del datore di lavoro, garantendo a tutti i cittadini il diritto al lavoro con l'art. 4 che dichiara: "La Repubblica riconosce a tutti i cittadini il diritto al lavoro e promuove le condizioni che rendano effettivo questo diritto. Ogni cittadino ha il dovere di svolgere, secondo le proprie possibilità e la propria scelta, una attività o una funzione che concorra al progresso materiale o spirituale della società.", tutela i diritti inviolabili dell'uomo con l'art. 2: "La Repubblica riconosce e garantisce i diritti inviolabili dell'uomo, sia come singolo, sia nelle formazioni sociali ove si svolge la sua personalità, e richiede l'adempimento dei doveri inderogabili di solidarietà politica, economica e sociale.", difende il diritto di uguaglianza con l'art. 3: "Tutti i cittadini hanno pari dignità sociale e sono eguali davanti alla leg-

ge, senza distinzione di sesso, di razza, di lingua, di religione, di opinioni politiche, di condizioni personali e sociali." e difende i diritti fondamentali della personalità con l'art. 13: "La libertà personale è inviolabile. Non è ammessa forma alcuna di detenzione, di ispezione o perquisizione personale, né qualsiasi altra restrizione della libertà personale, se non per atto motivato dall'Autorità giudiziaria e nei soli casi e modi previsti dalla legge. [...]", tutela la libertà e la segretezza della corrispondenza con l'art. 15: "La libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione sono inviolabili. La loro limitazione può avvenire soltanto per atto motivato dell'Autorità giudiziaria con le garanzie stabilite dalla legge." , la libertà di manifestazione del pensiero con l'art. 21: "Tutti hanno diritto di manifestare liberamente il proprio pensiero con la parola, lo scritto e ogni altro mezzo di diffusione. [...]", la libertà di organizzazione sindacale con l'art. 39: "L'organizzazione sindacale è libera. Ai sindacati non può essere imposto altro obbligo se non la loro registrazione presso uffici locali o centrali, secondo le norme di legge. [...]" e il diritto di sciopero con l'art. 40.

4.2 La tutela della riservatezza

Il diritto alla riservatezza è un diritto inviolabile che tutela la persona dall'intrusione di terzi nella sfera privata dell'individuo, mentre il diritto al segreto è un diritto relativo, che consiste nell'obbligo al silenzio imposto ad un persona, per evitare la divulgazione di una determinata notizia. Un fatto privato significa che la sua diffusione non crea un'utilità sociale, e che la collettività, con la conoscenza del fatto, non ricava nessun beneficio: nasce dunque, la tutela della riservatezza per evitare che la vita privata di un soggetto venga divulgata senza il suo consenso.
Nel rapporto di lavoro, dove è presente un intenso scambio di dati personali, vi è dunque un forte pericolo che il potere del datore di lavoro possa essere illecito nei confronti del dipendente. Il lavoratore però, con la stipulazione del contratto di lavoro, rinuncia a una parte della tutela alla propria riserva-

tezza nei confronti del medesimo. Vi sono dunque diversi limiti per garantire il diritto alla riservatezza: i limiti del Codice della privacy e dello Statuto dei lavoratori.[1]
E' interessante analizzare lo Statuto dei lavoratori per approfondire il concetto dei limiti del potere di controllo e la garanzia della tutela della riservatezza, infatti, di particolare importanza sono gli articoli 2, 3 e 4, che verranno descritti successivamente.

4.3 Il divieto di controllo da parte delle guardie giurate e da parte di ignoti

L'art. 2 dello Statuto dei lavoratori è diretto allo scopo di evitare un clima intimidatorio nella prestazione lavorativa. Il datore di lavoro può avvalersi del controllo di terzi secondo l'art. 2 della Legge n. 300, ma solo per scopi di tutela del patrimonio aziendale, e quindi alle guardie giurate è vietato l'accesso nei locali, dove i dipendenti stanno adempiendo alla propria attività lavorativa.
Congiunto all'articolo precedente, l'art. 3 sancisce che: "I nominativi e le mansioni specifiche del personale addetto alla vigilanza dell'attività lavorativa debbono essere comunicati ai lavoratori interessati." Il fine di questa norma è quello di evitare il controllo occulto, e garantisce alle guardie giurate l'accesso nei locali in cui si svolge l'attività lavorativa[2].
Secondo la giurisprudenza vi è una connessione tra l'art. 3 dello Statuto dei lavoratori e l'art. 2104 del Codice civile: "il potere del datore di lavoro ai sensi degli art. 2086 e 2104 c.c. di controllare direttamente o mediante l'organizzazione gerarchica che fa a lui capo e che conosciuta dai dipendenti, l'adempimento cui costoro sono tenuti e, quindi, di accertare eventuali

[1]Enrico Barraco - Andrea Sitzia, *La tutela della privacy nei rapporti di lavoro*, Ipsoa, 2008

[2]Franco Toffoletto, *Nuove tecnologie informatiche e tutela del lavoratore, il potere di controllo del datore di lavoro - il telelavoro*, Giuffrè editore, 2006

mancanze specifiche dei dipendenti medesimi già commesse o in corso di esecuzione". E' vietato quindi il controllo della prestazione da parte di soggetti ignoti, ma non è vietato il controllo occulto o a sorpresa da parte di soggetti abilitati a farlo e se la loro attività di controllo è nota al lavoratore.
La giurisprudenza ha voluto però legittimare alcune fattispecie nei casi di controllo difensivo, cioè quei controlli che vengono effettuati in modo occulto, ma a titolo occasionale e non continuativo e che sono indispensabili per la tutela del patrimonio aziendale[3].

4.4 Il divieto di controllo a distanza

Un altro importante limite posto al datore di lavoro è il mezzo con cui si possono effettuare i controlli che non devono essere lesivi della dignità e riservatezza del dipendente.
Per controllo a distanza "deve pacificamente intendersi sia quello effettuato in ambito topografico lontano dal lavoratore sia quello conseguibile in tempi non sincronici (e cioè differiti) con quelli dell'adempimento della prestazione. La dizione è comprensiva, quindi, di una nozione spaziale e di un'alternativa o concorrente nozione temporale. Talché, a quest'ultima stregua, risulta oggettivamente riconducibile alla fattispecie vietata (o condizionata all'accordo preclusivo delle R.s.a.) l'installazione di apparecchiature che, tramite la registrazione e memorizzazione di dati suscettibili di analisi o assemblaggio in tempi successivi, consentano al datore di lavoro un controllo "a posteriori" in ordine all'attività ed al comportamento dei lavoratori[4]".
L'art. 4 dello Statuto spiega l'utilizzo degli impianti audiovisivi per il controllo dei lavoratori: "E' vietato l'uso di impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori." Questo primo comma, è un divieto assoluto assistito da sanzione penale che

[3]Enrico Barraco - Andrea Sitzia, *La tutela della privacy nei rapporti di lavoro*, Ipsoa, 2008

[4]Conforme, in giurisprudenza, Pret. pen. Milano 5.12.1984, relativa alla Soc. Ibm, in Foro it., 1985, I, 286, con nota di Rossi.

viene seguito dal secondo comma, che invece è un divieto flessibile e consente l'installazione di apparecchiature per il monitoraggio: "Gli impianti e le apparecchiature di controllo che siano richiesti da esigenze organizzative e produttive ovvero dalla sicurezza del lavoro, ma dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori, possono essere installati soltanto previo accordo con le rappresentanze sindacali aziendali, oppure, in mancanza di queste, con la commissione interna."
La giurisprudenza ritiene antisindacale il comportamento del datore di lavoro, che effettua un controllo a distanza con impianti audiovisivi senza aver raggiunto un accordo con le rappresentanze dei lavoratori[5]. Per quanto riguarda la casistica giurisprudenziale si possono citare alcuni esempi: è stata ritenuta illegittima in giurisprudenza[6]l'installazione al centro dell'officina di un locale rialzato con pareti di vetro (destinato ad ufficio del Capo officina), in quanto, anche se ciò non è stato espresso apertamente, acquisiva di fatto e nella pratica la funzione di "torre di controllo" da cui il Capo officina poteva controllare a distanza l'attività dei lavoratori.
Un altro tipo di comportamento illecito sul controllo a distanza può essere l'installazione di tachigrafi sugli automezzi in dotazione di autisti, viaggiatori o piazzisti che ricade nella fattispecie del secondo comma dell'art. 4 dello Statuto dei lavoratori, che può essere considerato come un controllo "a posteriori" dell'attività dei lavoratori. Il Ministero del lavoro e della previdenza sociale, con risoluzione del 15 dicembre 1971[7]dispose che: "ove la ditta abbia effettuato l'installazione dei tachigrafi sugli automezzi dei piazzisti, con possibilità di utilizzazione secondaria di tali apparecchiature, quali mezzi tecnici per il controllo della costanza dell'impegno lavorativo del personale dipen-

[5]Enrico Barraco - Andrea Sitzia, *La tutela della privacy nei rapporti di lavoro*, Ipsoa, 2008

[6]Pret. Pen. Roma 3 ottobre 1973, in Or. giur. lav. 1973, 753, confermata da Trib. Pen. Roma 10 luglio 1974, ibidem 1975, 289.

[7]La risoluzione trovasi in Or. giur. lav. 1972, 28, adesiva all'orientamento già in precedenza espresso nei confronti della ditta Sitia Yomo srl dall'Ispettorato del lavoro di Milano in data 26 luglio 1971, ibidem 1971, 623. Conf. per i c.d. congegni Kienzle, Pret. Milano 4 ottobre 198, in Not. giurisp. lav. 1989, 436

dente, l'Ispettorato del lavoro è tenuto a provvedere, ai sensi dell'art. 4, terzo co., dello Statuto, alle appropriate eventuali prescrizioni per l'adeguamento e le modalità d'uso degli impianti suddetti, per evitare che essi possano essere utilizzati per controlli a distanza dell'attività dei lavoratori e che la ditta possa trarre dalle registrazioni relative indicazioni per eventuali provvedimenti a carico dei piazzisti".

Successivamente anche gli articoli 6 e 8 limitano il suddetto potere per quanto riguarda le visite personali di controllo. L'art. 6 dichiara: "Le visite personali di controllo sul lavoratore sono vietate fuorché nei casi in cui siano indispensabili ai fini della tutela del patrimonio aziendale, in relazione alla qualità degli strumenti di lavoro o delle materie prime o dei prodotti." e l'art. 8 vieta "al datore di lavoro, ai fini dell'assunzione, come nel corso dello svolgimento del rapporto di lavoro, di effettuare indagini, anche a mezzo di terzi, sulle opinioni politiche, religiose o sindacali del lavoratore, nonché su fatti non rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore.". Nel quinto capitolo verranno analizzate anche altre norme di tutela del lavoratore, che riguardano il trattamento dei dati personali e sono molto importanti per quanto riguarda il controllo che il datore di lavoro può effettuare sui computer dati in uso al dipendente.

Capitolo 5

Il trattamento dei dati personali

5.1 I dati personali, i dati sensibili e i dati anonimi

Durante la prestazione lavorativa vi è un intenso scambio di informazioni e di dati tra il datore di lavoro e il dipendente. Bisogna quindi capire in quale modo i dati possano venire trattati e utilizzati.
E' molto importante definire alcuni concetti fondamentali per comprendere al meglio i metodi leciti per il trattamento dei dati personali. Per trattamento dei dati si intende: "qualunque operazione o complesso di operazioni, effettuate anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati[1];".
Per dato personale si intende: "qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, an-

[1]Codice della privacy, Decreto legislativo 30 giugno 2003, n. 196

che indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;[2]".
Per "qualsiasi informazione" si intendono tutte le informazioni soggettive come opinioni o valutazioni, o oggettive come la presenza di una sostanza nel sangue di una persona. Per dato sensibile invece s'intende un dato che rivela "l'origine razziale o etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale[3]" di un soggetto. Il dato anonimo è quello che "in origine, o a seguito di un trattamento, non può essere associato ad un interessato identificato o identificabile[4]".

5.2 I soggetti del trattamento

Nell'art. 4, comma 1, del Codice della privacy vengono spiegate le definizioni delle figure che prendono parte al trattamento dei dati personali:

- "titolare", la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza;

- "responsabile", la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali;

- "incaricati", le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;

[2]Codice della privacy, Decreto legislativo 30 giugno 2003, n. 196
[3]Codice della privacy, Decreto legislativo 30 giugno 2003, n. 196
[4]Codice della privacy, Decreto legislativo 30 giugno 2003, n. 196

- "interessato", la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali;

Il titolare, quindi, è il soggetto con il potere decisionale sui dati, il responsabile è il soggetto nominato per mansioni di coordinamento o esecutive e l'art. 29 del Codice della privacy, comma 4, prevede che i compiti affidati al responsabile siano analiticamente specificati per iscritto. Il responsabile si assume anche i rischi della gestione dei dati e la responsabilità per il trattamento illecito dei medesimi nel caso di mancato rispetto delle istruzioni del titolare, ma non elimina l'eventuale coinvolgimento risarcitorio del titolare[5]. L'incaricato è invece il soggetto che opera sui dati personali per conto del responsabile.

5.3 Informativa e consenso al trattamento dei dati personali

Per poter utilizzare, raccogliere ed elaborare i dati di un soggetto, quest'ultimo deve manifestare il suo consenso, informato ed espresso liberamente. I dati personali, che possono essere utilizzati devono essere:

- trattati in modo lecito e secondo correttezza;
- raccolti e registrati per scopi determinati, espliciti e legittimi ed utilizzati in modo compatibile con altri scopi;
- esatti ed aggiornati;
- pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati;

[5]Enrico Barraco - Andrea Sitzia, *La tutela della privacy nei rapporti di lavoro*, Ipsoa, 2008

- conservati in una forma che consenta l'identificazione dell'interessato per un periodo non superiore a quello necessario per gli scopi per cui i dati sono stati raccolti e trattati[6].

L'interessato deve aver preso visione dell'informativa, che contiene una serie di indicazioni sui metodi, le tipologie di operazioni che verranno effettuate sui dati. Secondo l'art. 13 del Codice della privacy l'informativa può essere orale o scritta e deve essere previa rispetto al trattamento dei dati. L'interessato deve quindi essere informato circa:

a) le finalità e le modalità del trattamento cui sono destinati i dati;

b) la natura obbligatoria o facoltativa del conferimento dei dati;

c) le conseguenze di un eventuale rifiuto di rispondere;

d) i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o di cui possono venire a conoscenza in qualità di responsabili o incaricati, e l'ambito di diffusione dei dati medesimi;

e) i diritti dell'interessato;

f) gli estremi identificativi del titolare e, se designati, del rappresentante. Quando il titolare ha designato più responsabili, è indicato almeno uno di loro, indicando il sito della rete di comunicazione o le modalità attraverso le quali è conoscibile in modo agevole l'elenco aggiornato dei responsabili[7].

Dopo aver preso visione dell'informativa, l'interessato darà il consenso al trattamento dei dati personali che deve essere espresso liberamente. "Espresso liberamente" significa che: " si presenta come manifestazione del diritto dell'autodeterminazione informativa, e dunque al riparo da qualsiasi pressione

[6]Codice della privacy, Decreto legislativo 30 giugno 2003, n. 196
[7]Codice della privacy, Decreto legislativo 30 giugno 2003, n. 196

se non viene condizionato all'accettazione di clausole che determinino un significativo squilibrio dei diritti e degli obblighi derivanti dal contratto[8].".
Se i dati vengono raccolti e non vengono rispettati i presupposti per la validità del consenso, il trattamento dei dati è illecito. Un limite importante al potere del datore di lavoro sul trattamento dei dati viene imposto dall'art. 8 dello Statuto dei lavoratori che dichiara: "È fatto divieto al datore di lavoro, ai fini dell'assunzione, come nel corso dello svolgimento del rapporto di lavoro, di effettuare indagini, anche a mezzo di terzi, sulle opinioni politiche, religiose o sindacali del lavoratore, nonché su fatti non rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore.".
Vi sono casi però, in cui è lecito il trattamento dei dati senza il consenso espresso dell'interessato, e vengono descritti nel Codice della privacy nell'art. 24: "Il consenso non è richiesto quando il trattamento:

a) è necessario per adempiere ad un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria;

b) è necessario per eseguire obblighi derivanti da un contratto del quale è parte l'interessato o per adempiere, prima della conclusione del contratto, a specifiche richieste dell'interessato;

c) riguarda dati provenienti da pubblici registri, elenchi, atti o documenti conoscibili da chiunque, fermi restando i limiti e le modalità che le leggi, i regolamenti o la normativa comunitaria stabiliscono per la conoscibilità e pubblicità dei dati;

d) riguarda dati relativi allo svolgimento di attività economiche, trattati nel rispetto della vigente normativa in materia di segreto aziendale e industriale;

e) è necessario per la salvaguardia della vita o dell'incolumità fisica di un terzo. Se la medesima finalità riguarda l'interessato e quest'ultimo non può prestare il proprio consenso per impossibilità fisica, per incapacità

[8]Garante per la protezione dei dati personali, provvedimento del 28 maggio 1997

di agire o per incapacità di intendere o di volere, il consenso è manifestato da chi esercita legalmente la potestà, ovvero da un prossimo congiunto, da un familiare, da un convivente o, in loro assenza, dal responsabile della struttura presso cui dimora l'interessato. Si applica la disposizione di cui all'articolo 82, comma 2;

f) con esclusione della diffusione, è necessario ai fini dello svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397, o, comunque, per far valere o difendere un diritto in sede giudiziaria, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento, nel rispetto della vigente normativa in materia di segreto aziendale e industriale;

g) con esclusione della diffusione, è necessario, nei casi individuati dal Garante sulla base dei principi sanciti dalla legge, per perseguire un legittimo interesse del titolare o di un terzo destinatario dei dati, anche in riferimento all'attività di gruppi bancari e di società controllate o collegate, qualora non prevalgano i diritti e le libertà fondamentali, la dignità o un legittimo interesse dell'interessato;

h) con esclusione della comunicazione all'esterno e della diffusione, è effettuato da associazioni, enti od organismi senza scopo di lucro, anche non riconosciuti, in riferimento a soggetti che abbiano con essi contatti regolari o ad aderenti, per il perseguimento di scopi determinati e legittimi individuati dall'atto costitutivo, dallo Statuto o dal contratto collettivo, e con modalità di utilizzo previste espressamente con determinazione resa nota agli interessati all'atto dell'informativa ai sensi dell'articolo 13;

i) è necessario, in conformità ai rispettivi codici di deontologia di cui all'allegato A), per esclusivi scopi scientifici o statistici, ovvero per esclusivi scopi storici presso archivi privati dichiarati di notevole interesse storico ai sensi dell'articolo 6, comma 2, del decreto legislativo 29 ottobre

> 1999, n. 490, di approvazione del testo unico in materia di beni culturali e ambientali o, secondo quanto previsto dai medesimi codici, presso altri archivi privati."

Per quanto riguarda il consenso, deve essere comunque richiesto in caso di dati sensibili. E' possibile trattare i dati sensibili senza consenso, ma previa autorizzazione del Garante con il consenso scritto dell'interessato e quando il trattamento è "necessario per adempiere a specifici obblighi o compiti previsti dalla legge, da un regolamento o dalla normativa comunitaria per la gestione del rapporto di lavoro, anche in materia di igiene e sicurezza del lavoro e della popolazione, di previdenza e assistenza, nei limiti previsti dall'autorizzazione e ferme restando le disposizioni del codice di deontologia e di buona condotta di cui all'art. 111 del Codice[9].".
Per unire il discorso sul trattamento dei dati con il potere di controllo del datore di lavoro, basti pensare alla decisione del Garante della privacy del 2 febbraio 2006, adottata a "seguito di un ricorso presentato da un lavoratore a cui il datore di lavoro aveva contestato disciplinarmente la navigazione in siti Internet a contenuto religioso, politico e pornografico, durante l'orario di lavoro, allegando alla lettera di contestazione l'elenco dettagliato di tali siti. Per contestare l'indebito utilizzo dei beni aziendali, afferma il Garante, sarebbe stato sufficiente verificare gli avvenuti accessi ad Internet ed i tempi di connessione senza indagare sui contenuti dei siti visitati[10].".

5.4 Il Codice sulla privacy

Il decreto legislativo n.196 del 2003 può essere considerato come "il primo tentativo, su scala internazionale, di riordino generale di una materia complessa e, soprattutto, straordinariamente mobile. E' strutturato secondo

[9]Garante per la protezione dei dati personali, Autorizzazione n. 1/2005 al trattamento dei dati sensibili nei rapporti di lavoro - 21 dicembre 2005

[10]Franco Toffoletto, *Nuove tecnologie informatiche e tutela del lavoratore, il potere di controllo del datore di lavoro - il telelavoro*, Giuffrè editore, 2006

moduli diversi, ma ha un impianto nel quale assume specifica rilevanza la trama dei principi[11]". Il Codice sulla privacy ha portato numerose modifiche nella regolamentazione della materia sul trattamento dei dati personali, completando la direttiva 95/46/CE e raccoglie in un testo unico la legge n.675 del 31 dicembre 1996[12]e le altre fonti legislative, che si sono succedute negli anni[13].

Il codice della privacy è diviso in tre parti: la prima parte (artt. 1-45) contiene disposizioni applicabili a qualsiasi tipo di trattamento, la seconda parte (artt. 46 - 140) contiene disposizioni speciali volte a disciplinare i trattamenti di dati personali in specifici settori, infine la terza parte contiene disposizioni relative alla tutela dell'interessato e le sanzioni[14].

Il sistema delle fonti normative che tutela la sfera personale del lavoratore in Italia sono diverse, e il Codice della privacy deve confrontarsi con altre normative già vigenti, come gli art. 2,3,4,5,6 e 8 dello Statuto dei Lavoratori e con le norme del codice civile. Per togliere ogni incertezza l'art. 184, comma 3, dispone che "restano ferme le disposizioni di legge o di regolamento che stabiliscono divieti o limiti più restrittivi in materia di trattamento di taluni dati personali.". Il Codice sulla privacy si aggiunge quindi alla disciplina vigente e rinvia ad altre leggi applicabili come l'art. 8 dello Statuto dei lavoratori nell'art. 112, e l'adozione di particolari atti nell'art. 111. Nel Codice è presente anche un'importante analisi dei compiti del Garante per la protezione dei dati personali nell'art. 153 e 154. Uno di questi compiti è quello di "segnalare al Parlamento e al Governo l'opportunità di interventi normativi richiesti dalla necessità di tutelare i diritti", come sta avvenendo in questo momento in cui mancano normative per quanto riguarda il potere

[11]S.Rodotà, Tra diritti fondamentali ed elasticità della normativa: il nuovo Codice sulla privacy, in Eur. dir. Privato, 2004, 1 ss.

[12]La legge n.675, del 1996 contiene una disciplina generale sulla tutela della privacy nel trattamento dei dati personali.

[13]Enrico Barraco - Andrea Sitzia, *La tutela della privacy nei rapporti di lavoro*, Ipsoa, 2008

[14]Enrico Barraco - Andrea Sitzia, *La tutela della privacy nei rapporti di lavoro*, Ipsoa, 2008

di controllo sui lavoratori in ambito informatico.

Capitolo 6

Nuove tecnologie per il monitoraggio dei lavoratori

6.1 La tecnologia RFID

L'evoluzione tecnologica, per quanto riguarda il monitoraggio e la prevenzione di intrusioni, offre soluzioni che riducono al minimo questo tipo di problema, ma spesso queste tecnologie, come la tecnologia Rfid, possono aggredire la privacy di un individuo. La tecnologia Rfid (Radio Frequency ID Devices) utilizza dispositivi microscopici quali i microchip, che contengono un identificativo come un numero di serie e vengono letti da lettori compatibili in radiofrequenza.[1]
Secondo la definizione del Garante contenuta nella Newsletter n. 243 del 31 gennaio 2006 i principali componenti di un sistema Rfid sono: "Un tag, ossia un circuito elettronico miniaturizzato che contiene memorizzate alcune informazioni ed è unito ad un'antenna in grado di comunicare queste informazioni attraverso onde radio; un lettore (dotato a sua volta di un'antenna di trasmissione/ricezione); un decodificatore che traduce i dati in entrata in dati digitali potenzialmente trattabili da un computer.".

[1]Diritto dell'internet e delle nuove tecnologie telematiche, G.Cassano - I.P Cimino, Cedam, 2009

L'uscita di questa nuova tecnologia suscitò nelle maggiori imprese grande interesse, in quanto questo sistema può essere impiegato in numerosi settori: per tracciare i movimenti di una singola unità di prodotto nella catena di distribuzione, per la prevenzione di furti e per controllare le aree riservate. Il problema del sistema Rfid sorge "quando alcuni impieghi di questa tecnologia, che non si limitino a tracciare il prodotto per garantire l'efficienza del processo di produzione industriale, possono costituire una violazione del diritto alla protezione dei dati personali e determinare forme di controllo sulle persone: con l'uso di Rfid si potrebbero, infatti, raccogliere innumerevoli dati sulle abitudini dei consumatori al fine di profilazione o si potrebbe essere in grado di tracciare i percorsi effettuati dagli stessi, controllarne la posizione geografica o verificare quali prodotti usano, indossano, trasportano.
I sistemi Rfid possono essere usati, inoltre, da soggetti pubblici o privati anche per altri scopi, quali l'identificazione personale o la tutela della salute. Alcuni particolari usi, come l'impianto di microchip sottopelle, sollevano ormai problematiche di grande delicatezza che hanno già indotto altre autorità garanti in Europa a considerarli inaccettabili sul piano della protezione dei dati personali."
Un altro problema possibile è quello che può verificarsi con l'aumento della potenza del sistema Rfid: i dati contenuti nelle "etichette intelligenti" potrebbero essere letti o modificati da terzi non autorizzati. Occorre quindi tenere conto dei problemi che questo sistema di monitoraggio può avere sui diritti delle persone e sulla protezione dei dati personali[2].
Il Garante, per far fronte a questa problematica, ha precisato l'utilizzo delle tecnologie Rfid con il provvedimento n. 249 del 2005, dichiarando che qualora l'utilizzo delle tecnologie Rfid comporti il trattamento di dati personali "le persone devono essere adeguatamente informate dell'utilizzo di sistemi Rfid, così come dell'esistenza dei lettori ottici che attivano l'etichetta. La presenza di avvisi nei luoghi nei quali le tecniche Rfid sono utilizzate non esime da

[2]Diritto dell'internet e delle nuove tecnologie telematiche, G.Cassano - I.P Cimino, Cedam, 2009

apporre informativa sugli stessi oggetti e prodotti che recano le etichette intelligenti." e "Un soggetto privato che utilizza Rfid trattando dati personali può farlo solo con il consenso espresso e specifico degli interessati, a meno che ricorra in casi particolari uno degli altri presupposti di legge. Il consenso non è valido se ottenuto con pressioni o condizionamenti sull'interessato."
Per quanto riguarda invece i più invasivi sistemi Rfid sottopelle il Garante ha dichiarato che: "Tali impianti devono ritenersi in via di principio esclusi in quanto in contrasto con i diritti, le libertà fondamentali e la dignità della persona. Essi possono essere ammessi solo in casi eccezionali per comprovate e giustificate esigenze di tutela della salute delle persone. L'interessato, comunque, deve poter ottenere la rimozione del microchip e l'interruzione del relativo trattamento dei dati che lo riguardano. Si devono prevedere modalità di impianto che garantiscano la riservatezza circa la presenza delle etichette nel corpo dell'interessato.
Va ricordato che anche nei casi di un limitato impiego di microprocessori sottocutanei (es. Stati Uniti), sono stati messi in evidenza i potenziali rischi sia per la salute dei soggetti che si sottopongono all'impianto, sia per la sicurezza dei dati personali trattati.
Il Garante ha stabilito, comunque, che i soggetti che intendono utilizzare tali microchip devono sottoporre alla verifica preliminare dell'Autorità tali sistemi.".

Capitolo 7

Analisi delle policy aziendali del CUP 2000 di Bologna, dell'Ente Regione Emilia Romagna e dell'Università di Bologna

In questo capitolo verranno analizzate le policy aziendali del CUP 2000 di Bologna, dell'Ente Regione Emilia Romagna e dell'Università di Bologna per approfondire il concetto di tutela del patrimonio aziendale, il potere di controllo del datore di lavoro e la tutela dei diritti del lavoratore.

7.1 Policy aziendale del CUP 2000 di Bologna

Il Cup 2000 di Bologna offre la possibilità di accedere alle prestazioni sanitarie e ai servizi ambulatoriali e diagnostici presenti sul territorio di Bologna e provincia. L'azienda ha una struttura a matrice, cioè l'impresa è

organizzata in modo tale che la divisione del lavoro direttivo sia effettuata in base ad un sistema di comando multiplo. Per tutelare la propria sicurezza e per informare il dipendente su eventuali norme da seguire, è stata stilata una precisa e completa policy aziendale. Per quanto riguarda i problemi che si possono creare nella sfera di Internet, sono state imposte determinate regole da seguire onde evitare danni aziendali.

L'introduzione della policy verte sull'utilizzo della tecnologia messa a disposizione dei dipendenti e la relativa modalità di utilizzo della medesima e affronta il discorso in modo netto e chiaro "L'Azienda mette a disposizione dei lavoratori una serie di risorse tecnologiche finalizzate alla produttività aziendale che costituiscono un costo per l'Azienda stessa. Per questo motivo ne sono vietati tutti gli utilizzi non in conformità con gli scopi dell'Azienda.". Per quanto riguarda l'utilizzo personale del computer, non possono essere installati ed utilizzati programmi senza autorizzazione e vi è un importante paragrafo in cui si avverte il dipendente della possibilità di ispezioni: "L'utente si impegna inoltre a consentire l'eventuale ispezione (nel rispetto della presente politica di gestione e della riservatezza dei dati personali e delle norme in vigore) del computer ricevuto in uso e dell'ambiente informatico in cui si trova.". In questo caso però, non viene fornita una descrizione dettagliata sulle modalità di controllo che potrebbero essere effettuate. Per quanto riguarda il danneggiamento del sistema informatico aziendale vi è una certa flessibilità: "In caso di malfunzionamento ovvero di danneggiamento dei beni aziendali l'interessato è tenuto a darne tempestivamente comunicazione se possibile scritta al Servizio Tecnico. Per quanto non specificato nel presente documento è richiesto comunque un atteggiamento ispirato alla correttezza ed alla buona fede. In ogni caso l'Amministratore di sistema provvederà a prendere opportune precauzioni tecnologiche secondo le norme sopraelencate.".

Di molta importanza e di particolare interesse è l'informativa sul monitoraggio del dipendente: "L'Azienda non intende monitorare l'utilizzo della rete in sé da parte dell'utente, ma si riserva il diritto di mantenere i log

del firewall e del proxy e di potersi così assicurare dell'utilizzo appropriato dell'infrastruttura da parte degli utenti, facendo osservare le sanzioni di cui al punto precedente, fermo restando l'obbligo di segnalare alla competente Autorità Giudiziaria ogni possibile violazione costituente reato.". Vengono memorizzate solamente le informazioni sulla postazione dove vi è stato un comportamento illecito, il tempo e gli orari di utilizzo, evitando di cadere così nella violazione del trattamento dei dati personali del dipendente. Successivamente, viene redatta una lista sui comportamenti vietati al dipendente per quanto riguarda l'utilizzo di Internet: "

1. il download o la condivisione di qualsiasi tipologia di file tramite programmi peer to peer (eMule, BitTorrrent, ShareAza, WinMX sono alcuni dei programmi peer to peer attualmente più diffusi. Tali programmi si appoggiano a protocolli comuni, è possibile quindi utilizzare programmi differenti da quelli elencati per accedere alla stessa rete peer to peer), ovvero tramite qualsiasi altro programma non autorizzato dal Servizio Tecnico per lo scambio di file tramite Internet;

2. la navigazione nel Web o l'uso di servizi che si appoggino a Internet senza software antivirus, o con il software antivirus bloccato o non adeguatamente aggiornato;

3. il download di file video, musicali ed eseguibili, salvo quando espressamente autorizzati dal Servizio Tecnico e solo per esigenze lavorative;

4. l'accesso e la navigazione su siti a carattere erotico-pornografico, casinò virtuali, webchat in Java, siti di tipo Warez e simili;

5. la modifica non autorizzata delle impostazioni di rete (ad esempio firewall di Windows, impostazioni del proxy, impostazione di DNS differenti da quelli impostati dal Servizio Tecnico, ecc.);

6. l'esecuzione di programmi di accesso e controllo remoto della propria postazione (ad esempio VNC, Desktop remoto e Assistenza remota in

Windows), sia dall'esterno, sia dall'interno, salvo esplicita autorizzazione;

7. la connessione ad Internet attraverso un qualsiasi altro mezzo che non sia la rete aziendale (ad esempio tramite linea telefonica analogica, tramite cellulare GPRS, EDGE, UMTS tramite connessioni WIFI, ecc.) salvo esplicita autorizzazione.

Per quanto non specificato nel presente documento è richiesto comunque un atteggiamento ispirato alla correttezza ed alla buona fede. In ogni caso il Responsabile dei Sistemisti provvederà a prendere opportune precauzioni tecnologiche a livello di firewall secondo le norme sopraelencate. L'utente si impegna inoltre a consentire l'eventuale ispezione (nel rispetto della presente politica di gestione e della riservatezza dei dati personali e delle norme in vigore) del computer ricevuto in uso e dell'ambiente informatico in cui si trova.".

In questo modo vengono scongiurati diversi comportamenti che limiterebbero la prestazione lavorativa del dipendente. Il Cup 2000 di Bologna, oltre la policy aziendale, impiega diversi metodi per impedire ai lavoratori gli utilizzi illeciti citati precedentemente: gli operatori di sportello che hanno a disposizione un computer, possiedono dei software installati per svolgere esclusivamente la propria prestazione lavorativa, e un collegamento ad Internet che viene filtrato da una whitelist, tramite la quale gli operatori potranno accedere solamente ai siti indicati nella lista. Al contrario, ai livelli superiori i dipendenti hanno più libertà e flessibilità, in quanto, Internet sarà filtrato da una blacklist impedendo l'accesso solo a determinati siti. Questi filtri, seguono le disposizioni del Garante della privacy nella deliberazione del 1° marzo 2007, n. 13, al paragrafo 5.2 punto a) "Internet: la navigazione web", che dichiara: "configurazione di sistemi o utilizzo di filtri che prevengano determinate operazioni reputate inconferenti con l'attività lavorativa quali l'upload o l'accesso a determinati siti (inseriti in una sorta di blacklist) e/o il download di file o software aventi particolari caratteristiche (dimensionali o di tipologia di dato);".

Per quanto riguarda i software per comunicare come Messenger e Skype non ci sono filtri o blocchi, in quanto sono indispensabili ai fini lavorativi, per contattare clienti e fornitori. Per contrastare la possibilità che il lavoratore passi troppo tempo a "distrarsi", piuttosto che nell'espletare la propria attività lavorativa non ci sono particolari imposizioni, a parte quella di avere dei limiti di tempo per ogni progetto o attività da svolgere, quindi il lavoratore dovrà essere in grado di autogestirsi per riuscire a terminare il compito assegnatogli entro un determinato periodo di tempo. Per la posta elettronica, oltre che per gli stessi accorgimenti che vengono elencati sull'utilizzo della navigazione nel web, vengono descritte altre forme di comportamento ritenute inopportune e viene utilizzato un software che previene malware e spam attraverso diversi livelli di filtro. Inizialmente, al primo livello i software utilizzati identificano lo spam, al secondo livello viene smistata la posta in arrivo dallo spam mentre nel terzo livello vi è un altro software che rileva i falsi positivi. Un interessante spazio è dedicato inoltre all'accesso della posta elettronica in caso di assenza prolungata dell'utente intestatario; si nota quindi, che vengono seguite precisamente le linee guida del Garante della privacy del 1° marzo 2007 che dichiarano: "il datore di lavoro metta a disposizione di ciascun lavoratore apposite funzionalità di sistema, di agevole utilizzo, che consentano di inviare automaticamente, in caso di assenze (ad es., per ferie o attività di lavoro fuori sede), messaggi di risposta contenenti le "coordinate" (anche elettroniche o telefoniche) di un altro soggetto o altre utili modalità di contatto della struttura." e infatti nella policy viene stabilito che: "In caso di assenza prolungata è consigliabile impostare il servizio di auto risposta.", ma viene presa in considerazione raramente e per casi eccezionali l'ipotesi di delegare un fiduciario per visionare la posta elettronica e sempre con il consenso espresso, o se possibile, in presenza del diretto interessato.

7.2 Policy aziendale dell'Ente Regione Emilia Romagna

La policy aziendale dell'Ente Regione Emilia Romagna è molto dettagliata, approfondita e divisa in diversi disciplinari tecnici, che regolano il comportamento dei dipendenti in diversi contesti come il controllo degli accessi ai locali e la sicurezza delle applicazioni informatiche nella Giunta della Regione Emilia-Romagna.
Per rimanere in tema del potere di controllo del datore di lavoro, il disciplinare tecnico n° 6928 del 21/07/2009 descrive come vengono effettuate verifiche periodiche sui sistemi informativi per "preservare la riservatezza, l'integrità e la disponibilità dei dati e delle informazioni; per garantire il rispetto di leggi e regolamenti in materia di protezione dei dati personali, in particolare dei requisiti minimi di sicurezza previsti dalla normativa vigente.
Le verifiche consistono in un'attività di monitoraggio sulla conformità dei sistemi informativi e dei comportamenti dei soggetti.". Questi controlli vengono effettuati secondo le norme vigenti e tenendo conto nello specifico del decreto legislativo 196/2003 "Codice in materia di protezione dei dati personali". Vengono citate successivamente le modalità di verifica:

a) puntuali preventive;
attività di verifica effettuate precedentemente all'implementazione o modifica sostanziale di un sistema o processo per verificarne la rispondenza alle politiche di sicurezza.

b) puntuali a posteriori;
attività di verifica effettuate a seguito del verificarsi di incidenti di sicurezza.

c) periodiche;
attività di verifica, manuali o automatizzate, per contrastare minacce incombenti o potenziali, effettuate con cadenza periodica programmata.

d) a campione.

attività di verifica effettuate su campioni scelti secondo criteri prestabiliti e ad intervalli di tempo non fissi.

Le verifiche di sicurezza possono essere effettuate esclusivamente da personale preventivamente autorizzato. L'autorizzazione è data in forma scritta dal Responsabile della sicurezza della Giunta o dal Responsabile della sicurezza dell'Assemblea Legislativa, ciascuno per la propria area di competenza. Qualora l'effettuazione delle verifiche comprenda il trattamento di dati personali, gli addetti devono essere preventivamente individuati quali incaricati del trattamento dal soggetto competente.
Di particolare interesse è il metodo di controllo applicato dall'Ente, infatti "l'Ente ritiene che l'attività di prevenzione debba essere prevalente rispetto all'attività di controllo. Si impegna pertanto a potenziare in misura crescente tale attività di prevenzione, in particolare tramite l'adozione di appositi disciplinari tecnici, azioni di sensibilizzazione e di diffusione dei principi e delle regole nell'utilizzo delle strumentazioni telematiche e telefoniche (ad esempio tramite comunicazioni interne e la predisposizione e diffusione di opuscoli informativi), attività formative mirate, specifiche soluzioni tecnologiche ed ogni altra misura ritenuta idonea a tal fine." L'Ente definisce poi 5 principi per effettuare i controlli: "il principio di necessità: i dati trattati durante l'attività di controllo devono essere sempre e soltanto quelli strettamente necessari; il principio di proporzionalità: i controlli devono sempre essere effettuati con modalità tali da garantire, nei singoli casi concreti, la pertinenza e non eccedenza delle informazioni rilevate rispetto alle finalità perseguite." Questi principi sono in linea con l'art. 11 del Decreto legislativo 30 giugno 2003, n. 196 che sancisce le modalità di trattamento dei dati personali, e i dati trattati devono essere: pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati.
"Il principio di imparzialità: i controlli devono essere effettuati su tutte le strumentazioni informatiche e telefoniche messe a disposizione dall'amministrazione regionale e conseguentemente possono coinvolgere tutti gli utiliz-

zatori delle stesse, a qualunque titolo abbiano assegnata la strumentazione. L'imparzialità inoltre deve essere garantita mediante sistemi automatici di estrazione casuale per l'effettuazione dei controlli a campione ed in nessun caso possono essere effettuati controlli mirati e ripetuti nei confronti di soggetti specifici con finalità discriminatorie o persecutorie o volutamente sanzionatorie." Questo principio segue le linee guida del Garante della privacy sul trattamento di dati che deve essere in forma anonima, tale da precludere l'immediata identificazione di utenti mediante loro opportune aggregazioni; "il principio di trasparenza: in base a tale principio l'amministrazione deve mettere in atto tutte le azioni necessarie per garantire la preventiva conoscenza da parte di tutti i soggetti potenzialmente sottoposti ai controlli del presente disciplinare. Devono pertanto essere informati dei possibili controlli tutti i soggetti che operano, a qualunque titolo e con qualunque rapporto, per l'Ente, tra cui, in particolare, tutti i soggetti che hanno con lo stesso sia un rapporto di lavoro subordinato (di qualsiasi tipologia) sia un rapporto di lavoro autonomo.", questo è un altro principio importante, in quanto segue le direttive dell'art. 13 del Decreto legislativo 30 giugno 2003, n. 196 sull'informativa dell'interessato e sul trattamento dei dati; e infine l'ultimo principio riguarda la " protezione dei dati personali: i controlli devono in ogni caso essere effettuati rispettando la dignità e la libertà personale dei soggetti sottoposti a controllo nonché garantendo la riservatezza dei dati personali raccolti durante la procedura di controllo."

Le verifiche e i controlli eseguiti dal personale designato sono effettuati secondo due modalità: puntuale e a campione. "Il controllo puntuale è effettuato su strumentazioni informatiche determinate, a seguito di specifica segnalazione effettuata da un soggetto terzo oppure in seguito ad una verifica di sicurezza."

"Il controllo a campione è effettuato, su strumentazioni informatiche non predeterminate, con cadenza trimestrale e con estrazione a sorte, mediante un generatore di numeri casuali, di una giornata nell'arco dei tre mesi precedenti all'estrazione. Il controllo è effettuato sui log di navigazione in Internet

relativi alla giornata estratta e ai 6 giorni successivi e consecutivi alla stessa giornata estratta.".
Queste due modalità di controllo seguono precisamente le normative riguardo al controllo da parte del datore di lavoro in quanto aderisce alla definizione di controllo difensivo, che è quel tipo di controllo a titolo occasionale, e non continuativo, indispensabile per la tutela del patrimonio aziendale e si attiene anche alle linee guida del Garante della privacy del 10 marzo 2007 in particolare al punto c) del paragrafo "Internet: la navigazione web", in cui si stabilisce che il datore di lavoro deve: "trattare i dati in forma anonima o tale da precludere l'immediata identificazione di utenti mediante loro opportune aggregazioni (ad es., con riguardo ai file di log riferiti al traffico web, su base collettiva o per gruppi sufficientemente ampi di lavoratori).", il controllo anonimo può concludersi con un avviso generalizzato relativo ad un uso inconsueto degli strumenti aziendali. Il garante prescrive, inoltre, che in caso di assenza di successive anomalie non è di regola giustificato effettuare controlli su base individuale.
Infine, in materia di corretto comportamento nell'utilizzo di strumenti informatici, l'Ente descrive un valido utilizzo dei medesimi: "Utilizzare l'accesso ad Internet, fornito dall'Ente per lo svolgimento dell'attività lavorativa, in modo pertinente alle specifiche finalità della propria attività, nel rispetto delle esigenze di funzionalità e di sicurezza della rete e dei sistemi. In particolare Internet può essere utilizzato per motivi personali in caso di urgenza e/o per il tempo strettamente necessario per assolvere incombenze amministrative e burocratiche quali adempimenti on line nei confronti di pubbliche amministrazioni ovvero per tenere rapporti con istituti bancari e assicurativi.
L'utilizzazione per motivi personali non deve essere comunque effettuata in modo ripetuto o per periodi di tempo prolungati.", e successivamente viene redatto un elenco completo, di facile comprensione, e ben dettagliato sui comportamenti ritenuti illeciti o non pertinenti alle specifiche finalità della propria attività, come: "

1. sono consultabili tutti i siti che siano visitati per motivi attinenti alla

propria attività lavorativa. Ad esempio, se si sta organizzando un convegno sull'agriturismo, si possono consultare tutti i siti agrituristici che servono; non si possono, al contrario, visitare ripetutamente gli stessi siti per organizzare una vacanza;

2. è sicuramente ammesso un collegamento per motivi personali e quindi un'utilizzazione dovuta a motivi di urgenza (quale può essere, ad es. una consultazione degli orari degli autobus o dei treni);

3. Non modificare le configurazioni standard del browser web o di altri software forniti dall'Ente.[...]"

Per quanto riguarda l'utilizzo della posta elettronica, dalla policy si deduce un comportamento generale che il dipendente deve mantenere per semplificare il problema nel caso in cui sia assente dal posto di lavoro e vi siano messaggi aziendali da dover consultare nella sua posta elettronica, il comportamento da tenere viene descritto in questo modo: " Prevedere opportune misure che consentano, in caso di assenza dal luogo di lavoro, ad altri utenti autorizzati l'accesso a dati potenzialmente necessari (per es. salvare i dati presenti sul proprio disco rigido in cartelle condivise su file server, utilizzare cartelle di Outlook condivise, utilizzare la funzione di delega di Outlook, ecc.).".
Nella Determinazione n. 2650/2007, viene descritto il caso in cui il soggetto assente può delegare il trattamento dei propri dati personali ad un altro soggetto (la delega può essere importante nel caso di assenza dell'interessato come detto precedentemente): "La richiesta può essere presentata anche da un soggetto terzo a cui l'interessato ha conferito, per iscritto, delega o procura, che agisce per conto dell'interessato, nell'esercizio dei diritti spettanti a quest'ultimo e cioè: - il delegato o procuratore dell'interessato (può trattarsi di persone fisiche o persone giuridiche, come ad esempio enti, organismi, associazioni, organismi portatori di interessi diffusi)."

7.3 Policy aziendale dell'Università di Bologna

L'università di Bologna offre un portale, consultabile liberamente, dove sono contenuti tutti i documenti e le normative che riguardano diversi settori: le elezioni, l'amministrazione, il personale, l'organizzazione, la ricerca e la privacy.
Per quanto riguarda la sfera del trattamento dei dati personali e il controllo del lavoratore, l'università ha stipulato il decreto rettorale N. 271/2009 del 23.02.2009 "Testo unico sulla privacy e sull'utilizzo dei sistemi informatici". Il decreto è formato da cinque parti, comprensive di quaranta articoli e quattro allegati. Il documento riporta diversi articoli tratti dal decreto legislativo 30 giugno 2003, n. 196, recante il "Codice in materia di protezione dei dati personali" e il provvedimento del Garante per la protezione dei dati personali del 1 marzo 2007; l'art. 7 è il primo articolo della seconda parte intitolata "Dati personali" e introduce l'argomento sulle modalità di trattamento dei succitati dati: "I sistemi informativi e i programmi informatici devono essere configurati riducendo al minimo l'utilizzazione di dati personali, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in casi di necessità." e, concludendo, la seconda parte riporta l'art. 11 del Codice della privacy che spiega il comportamento da mantenere per il trattamento dei dati del dipendente.
Vengono successivamente elencati i soggetti che prendono parte al trattamento dei dati descritti nell'art. 4, comma 1, del Codice della privacy e precedentemente riportati e descritti nel paragrafo 3.2, ed in seguito citate le sanzioni per comportamenti illeciti. Nella quarta parte, viene dichiarata anche la possibilità di effettuare controlli preventivi sul corretto uso e funzionamento degli strumenti informatici, nel rispetto dei diritti e delle libertà fondamentali dei lavoratori o dei soggetti esterni, che utilizzano strumenti

informatici dell'Ateneo, al fine di evitare usi impropri della rete o dei servizi di rete messi a disposizione dall'Ateneo.
In seguito viene redatta una lista sui casi in cui il controllo è ammesso: "

1. quando previsti da fonte normativa o regolamentare;
2. nel caso in cui si verifichino eventi dannosi o situazioni di pericolo non impediti da preventivi accorgimenti tecnici;
3. su segnalazione dell'Autorità Giudiziaria;
4. quando, per ragioni di continuità del servizio, sia indispensabile reperire dei file o dei messaggi di un lavoratore, secondo le modalità di cui al comma 5 del presente articolo;
5. nel caso in cui, nell'ambito delle ordinarie attività di gestione dei sistemi informativi di competenza, siano rilevati file illegali o dal contenuto palesemente non istituzionale;
6. nell'ambito di controlli saltuari a campione per le finalità di cui al comma 1."

Nei casi in cui, a seguito di un controllo, si rilevino comportamenti illegali o non istituzionali, il Ce.S.I.A. (Centro Servizi Informatici dell'Università di Bologna) o altri soggetti delegati dal Titolare potranno intervenire valutando se inviare avvisi collettivi o individuali in cui verranno segnalati i comportamenti non corretti e utilizzando in seguito dei possibili filtri onde evitare l'accesso a siti che non facciano parte della prestazione lavorativa. Nel comma 5 viene descritta la modalità di recupero dei file nel caso il lavoratore sia assente: "Il Responsabile di struttura, in caso di assenza prolungata di un lavoratore, anche quando dovuta al termine del periodo di collaborazione con l'Ateneo, e al fine di garantire la continuità lavorativa, chiede al Ce.S.I.A. di reperire i file di interesse per l'Ateneo giustificando adeguatamente i motivi della richiesta e informando per conoscenza il proprio lavoratore presso la propria residenza/domicilio eletto per le comunicazioni."; questo comma

segue le direttive dell'art. 13 comma 1 del Codice della privacy dove viene sancito che l'interessato deve essere informato circa le finalità e le modalità del trattamento cui sono destinati i dati.
Nell'allegato A, per garantire una maggiore sicurezza dei sistemi, viene dichiarato che non è consentito agli utenti di installare e utilizzare, nelle postazioni di lavoro, software illegali o software espressamente vietati dal proprio amministratore di sistema. Sempre nell'allegato A, nella terza parte vengono descritti i metodi di trattamento dei dati e le modalità di monitoraggio: "Qualunque struttura dell'Ateneo che, per obblighi di legge o di regolamenti, è tenuta al mantenimento dei log file (registri informatizzati che tengono traccia delle connessioni degli utenti e dei servizi a cui hanno avuto accesso), deve trattare tali dati conformemente alla normativa vigente e alle disposizioni fornite centralmente dal Ce.S.I.A." e successivamente viene ricordato che "la struttura ha l'obbligo di presentare all'interessato l'informativa relativa alla gestione dei dati di traffico. Ai sensi dell'art. 13 del decreto legislativo n. 196 del 30 giugno 2003". Nell' allegato C "Disciplinare per l'utilizzo della posta elettronica" viene descritto quale sia il comportamento idoneo nel caso di assenza programmata: "il dipendente è tenuto ad attivare sistemi di risposta automatica ai messaggi di posta elettronica ricevuti, nei quali indicherà eventuali indirizzi istituzionali alternativi ai quali fare riferimento per l'invio di comunicazioni.". Vengono infine descritte le modalità di utilizzo delle liste di distribuzione, cioè un indirizzo di posta elettronica, al quale viene associato un elenco di altri indirizzi. Quando un messaggio di posta elettronica viene inviato ad una lista di distribuzione, si ottiene come risultato la ricezione contemporanea dell'e-mail da parte di tutti gli indirizzi che sono compresi in quella lista. Queste liste di distribuzione sono soggette a controlli: "L'Ateneo può effettuare controlli a campione sulla legittimità del contenuto delle e-mail inviate mediante liste di distribuzione, al fine di verificarne l'aderenza alle disposizioni normative e alle prescrizioni contenute nel presente Regolamento" facendo riferimento quindi alla prima parte riguardo alle modalità e ai casi in cui il controllo è lecito.

Ringraziamenti

In questa pagina voglio ringraziare tutti coloro che mi hanno sostenuto in questi anni di Università:
Ringrazio innanzitutto la Professoressa Finocchiaro per tutti i consigli, l'aiuto e la disponibilità che mi ha rivolto in questi mesi.
Ringrazio il Professor Mollona per avermi aiutato ad integrare l'argomento della mia tesi con nozioni di economia.
Ringrazio il CUP 2000 di Bologna per avermi dato la possibilità di comprendere al meglio i vari problemi discussi nella mia tesi.
Grazie a Francesca, a Nerio e a Mariangela, che mi hanno aiutato pazientemente nella correzione della tesi.
Ringrazio di cuore Mariangela e Maurizio, i miei genitori, per aver avuto tanta pazienza in questi anni e per avermi sostenuto nonostante le numerose difficoltà.
Ringrazio tutti i miei nonni, Arvedo, Mirella e Marcella, i miei zii e cugini, perché con delle semplici parole, anche nei momenti peggiori mi hanno sempre donato un sorriso.
Voglio ringraziare, inoltre, tutti i miei compagni di Università per aver condiviso insieme gioie e dolori. In particolare ringrazio Tommy e Berny per tutte le giornate passate insieme a studiare e non, per tutte le difficoltà superate e per tutti i momenti in cui ci siamo davvero divertiti.
Un ringraziamento speciale va anche a Deza, amico di vecchia data, che mi ha supportato nello studio e mi ha aiutato a sostenere gli esami più complessi.
Ringrazio tutti i miei amici, che a loro modo hanno saputo starmi vicino in

ogni momento e con cui in questi anni mi sono divertito, annoiato, stupito, arrabbiato, giocato e intristito. Con voi ho passato momenti che non dimenticherò mai, grazie ragazzi.
E infine un ringraziamento particolare va ad Ilaria, che è riuscita a sopportarmi nei momenti più difficili e che ha sempre creduto in me. E' lei che ha condiviso più di ogni altro le mie gioie, ma soprattutto mi ha aiutato a superare diversi ostacoli apparentemente insormontabili. Grazie di cuore.

Luca, 13 luglio 2010